UNIVERSAL MANUAL / USERS MANUAL FOR: KY-8PSE30WM

KUSA

KY- 8PSE30WM

With

CYBER SECURE VIDEO

&

CLEAN CODE TECHNOLOGY

Power Over Ethernet (PoE)

(IEEE 802.3at) (IEEE 802.3az)

Industrial Managed Ethernet Switch

Universal User's Manual

Version 1.7, November 2011

Table of Contents

1.1 About the P.O.E SWITCH Industrial Switch 7
1.2 Software Features 7
1.3 Hardware Features 8

Cables 8
2.1 Ethernet Cables 8
2.1.1 100BASE-TX/10BASE-T Pin Assignments 9
2.2 SFP 11
2.3 Console Cable 11

WEB Management 12
3.1 Configuration by Web Browser 12
3.1.1 About Web-based Management 12
3.1.2 Basic Settings 14
3.1.2.1 System Information 14
3.1.2.2 Admin & Password 15
3.1.2.3 IP Address Setting 16
3.1.2.4 LLDP 17
3.1.2.5 Backup/Restore Configuration 21
3.1.2.6 Firmware Update 22
3.1.3 DHCP Server 22
3.1.3.1 Setting 22
3.1.3.2 DHCP Dynamic Client List 22
3.1.3.3 DHCP Client List 23
3.1.4 Port Setting 23
3.1.4.1 Port Control 23
3.1.4.2 Rate Limit 25
3.1.4.3 Port Trunk 26
3.1.5 Redundancy 31
3.1.5.1 Redundant Ring. 31
3.1.5.2 MSTP 33
3.1.6 VLAN 42
3.1.6.1 VLAN Membership Configuration 42
3.1.6.2 Private VLAN 43

3.1.7 SNMP 45

3.1.7.1 SNMP-System 45

3.1.7.2 SNMP-Communities 48

3.1.7.3 SNMP-Users 48

3.1.7.4 SNMP-Groups 50

3.1.7.5 SNMP-Views 51

3.1.7.6 SNMP-Accesses 52

3.1.8 Traffic Prioritization 53

3.1.8.1 Storm Control 53

3.1.8.2 Port Configuration 53

3.1.8.3 QoS Control List 54

3.1.8.4 QoS Statistics 56

3.1.8.5 Wizard 57

3.1.9 IGMP Snooping 57

3.1.9.1 IGMP Snooping 57

3.1.9.2 IGMP Snooping Status 59

3.1.10 Security 59

3.1.10.1 ACL 59

3.1.10.2 802.1x 68

3.1.11 Warning 82

3.1.11.3 Event Selection 84

3.1.12 Monitor and Diagnostics 85

3.1.12.1 MAC Table - Configuration 85

3.1.12.2 MAC Table - MAC Table- 87

3.1.13 Port Statistics 88

3.1.13.1 Traffic Overview 88

3.1.13.2 Detailed statistics 89

3.1.14 Port Monitoring 91

3.1.15 System Log Information 92

3.1.16 Cable Diagnostics 93

3.1.17 Ping 94

3.1.18 Power Over Ethernet (PoE) 95

3.1.18.1 PoE Configuration - Reserved Power determined 95

3.1.18.2 PoE Configuration - Power management Mode 96

3.1.18.3 PoE Configuration - Primary/backup Power Supply 97

3.1.18.4 PoE Configuration - Port Configuration 98

3.1.18.5 Power over Ethernet Status 99

3.1.18.6 LLDP Power Over Ethernet Neighbor 99

3.1.19 Factory Default 101

3.1.20 System Reboot 102

Command Line Interface Management 103

4.1 About CLI Management 103

COPYRIGHT NOTICE

Copyright © 2011 KUSA, LLC. All rights reserved.

No part of this publication may be reproduced in any form without the prior written consent of KUSA.

TRADEMARKS

KUSA is a registered trademark of KUSA. All other trademarks belong to their respective owners.

REGULATORY COMPLIANCE STATEMENT

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specifications section for more details.

WARRANTY

KUSA warrants that all KUSA products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). KUSA will repair or replace products found by KUSA to be defective within this warranty period, with shipment expenses apportioned by KUSA and the end user. This warranty does not cover product modifications or repairs done by persons other than KUSA-approved personnel, and this warranty does not apply to KUSA products that are misused, abused, improperly installed, or damaged by accidents. Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

DISCLAIMER

Information in this publication is intended to be accurate. KUSA shall not be responsible for its use or infringements on third-parties as a result of its use. There may occasionally be unintentional errors in this publication. KUSA reserves the right to revise the contents of this publication without notice.

KUSA CONTACT INFORMATION

KUSA

1107 SE Willow Pl, Blue Springs, MO 64014-5248

Website: www.KUSA1.co

Telephone: (219) 595 - 2631

(816) 988 - 7861

FAX: (480) 287 - 8605

Technical Support

E-mail: Sales@KUSA1.co

Sales Contact

E-mail: Sales@KUSA1.co (Headquarters)

Getting to Know Your Switch

1.1 About the P.O.E SWITCH Industrial Switch

The P.O.E SWITCH is powerful managed industrial switch which has many features. The switch can work under a wide range of temperatures, environments and humid conditions. The switch can be managed by WEB, TELNET and Console (Command Line) or other third-party SNMP software.

1.2 Software Features

- World's fastest Redundant Ethernet Ring (Recovery time < 10ms over 300 switches.
- Cyber-Secure Video with Clean Code Technology
- HD Camera Ready
- Supports Ring Coupling, Dual Homing, RSTP over Ring
- IGMP Snooping – IGMP v1/v2/v3
- Auto DOS/DDOS Protection (silicon based)
- Supports SNMPv1/v2c/v3 & RMON & Port base/802.1Q VLAN Network Management
- Event notification by Email, SNMP trap and Relay Output
- Windows Utility, Web-based ,Telnet and Console(CLI) configuration
- Enable/disable ports, MAC based port security
- Cyber Secure Video (CSV) with silicon enhancements for HD Video
- Port based network access control (802.1x)
- VLAN (802.1q) to segregate and secure network traffic
- Radius centralized password management
- SNMPv3 encrypted authentication and access security
- RSTP (802.1w)
- Quality of Service (802.1p) for real-time traffic
- VLAN (802.1q) with double tagging and GVRP supported
- IGMP Snooping for multicast filtering
- Port configuration, status, statistics, mirroring, security
- Remote Monitoring (RMON)

1.3 Hardware Features

- Operating Temperature: -40 to 80° C
- Storage Temperature: -40 to 85 ° C (-40 to 176º F)
- Operating Humidity: 5% to 95%, non-condensing
- Casing: IP-30
- 24 X 10/100/1000BaseT(X)
- 4 X 100/1000 Base(X) SFP Sockets
- Console Port

Cables

2.1 Ethernet Cables

The P.O.E switch has standard Ethernet ports. According to the link type, the switch uses CAT 3, 4, 5, 5e, or 6 UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	RJ-45
1000BASE-TX	Cat. 5-5e/Cat. 6 100-ohm UTP	UTP 100 m (328ft)	RJ-45

2.1.1 100BASE-TX/10BASE-T Pin Assignments

With 100BASE-TX/10BASE-T cabling, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

10/100 PSE Base-TX RJ-45 Pin Assignments (TYPE A) BA

Pin Number	Assignment
1	P.O.E Power input +
2	P.O.E Power input -
3	P.O.E Power input +
4	Not used
5	Not used
6	P.O.E Power input -
7	Not used
8	Not used

1000 Base-TX RJ-45 Pin Assignments

Pin Number	Assignment
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-

The P.O.E switch supports auto MDI/MDI-X operation. You can use a straight-through cable to connect PC to switch. The following table (below) shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

10/100 Base-TX MDI/MDI-X Pin Assignments

Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

1000 Base-TX MDI/MDI-X Pin Assignments

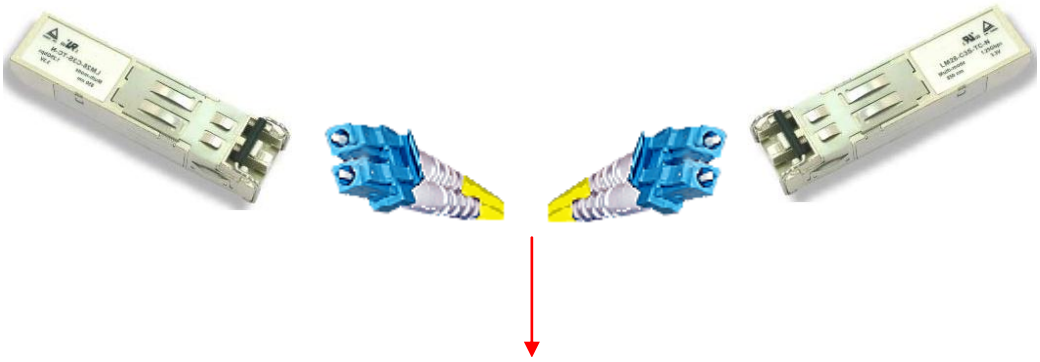
Pin Number	MDI port	MDI-X port
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

Note: "+" and "-" signs represent the polarity of the wires that make up each wire pair.

2.2 SFP

The Switch has small form factor (SFP) fiber optic port sockets for SFP modules. The fiber optic ports are in multi-mode (0 to 550M, 850 nm with 50/125 μm, 62.5/125 μm fiber) and single-mode with LC connector. Please remember that the TX port of Switch A should be connected to the RX port of Switch B.

Switch-A Switch-B

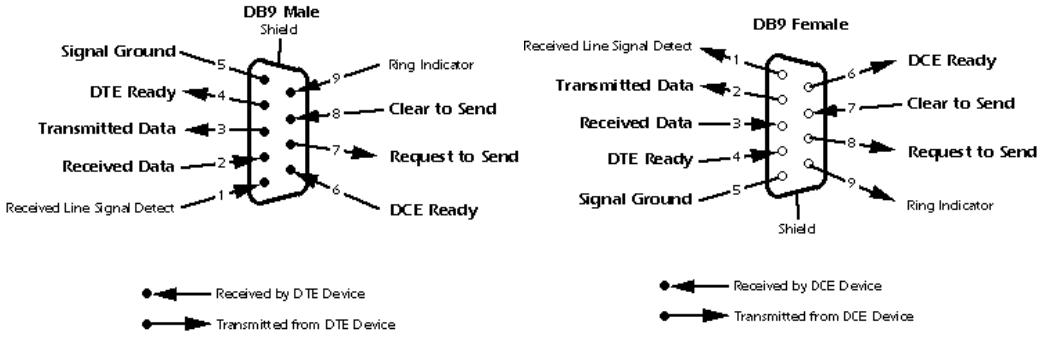


Fiber cord

2.3 Console Cable

The P.O.E SWITCH can be managed from its console port. The DB-9 to RJ-45 cable can be found in the packaging of your new equipment. You can connect the console port to PC via the RS-232 cable with DB-9 female connector and the other end (RJ-45 connector) connects to the console serial port of the switch.

PC pin out (male) assignment	RS-232 with DB9 female connector	DB9 to RJ 45
Pin #2 RD	Pin #2 TD	Pin #2
Pin #3 TD	Pin #3 RD	Pin #3
Pin #5 GD	Pin #5 GD	Pin #5



WEB Management

Warning!!!
While making any establishment and upgrading firmware, please remove physical loop connection first.
DO NOT power off equipment during firmware is upgrading!

3.1 Configuration by Web Browser

This section introduces the configuration by Web browser.

3.1.1 About Web-based Management

An embedded HTML web site resides in flash memory on the CPU board. It contains advanced management features and allows you to manage the switch from anywhere on the network through a standard web browser such as Microsoft IE, Google Chrome, or FireFox.

The Web-Based Management function supports Internet Explorer 5.0 or later. It is based on Java Applets with the aim to reduce network bandwidth consumption, enhance access speed and present an easy to use viewing screen.

Note: By default, IE5.0 or later version does not allow Java Applets to open sockets. You need to explicitly modify the browser setting in order to enable Java Applets to use the network ports.

Preparing for Web Management

The default values are defined below:

IP Address: **192.168.1.77 (Check Your Equipment Label to Insure a Match)**

Subnet Mask: **255.255.255.0**

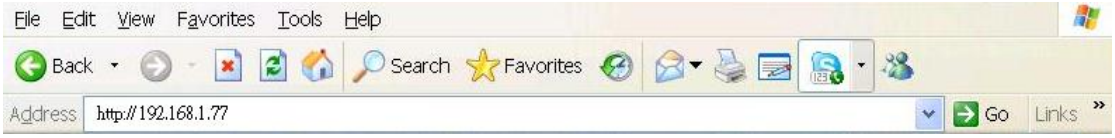
Default Gateway: **192.168.1.254**

User Name: **root**

Password: **root**

System Login

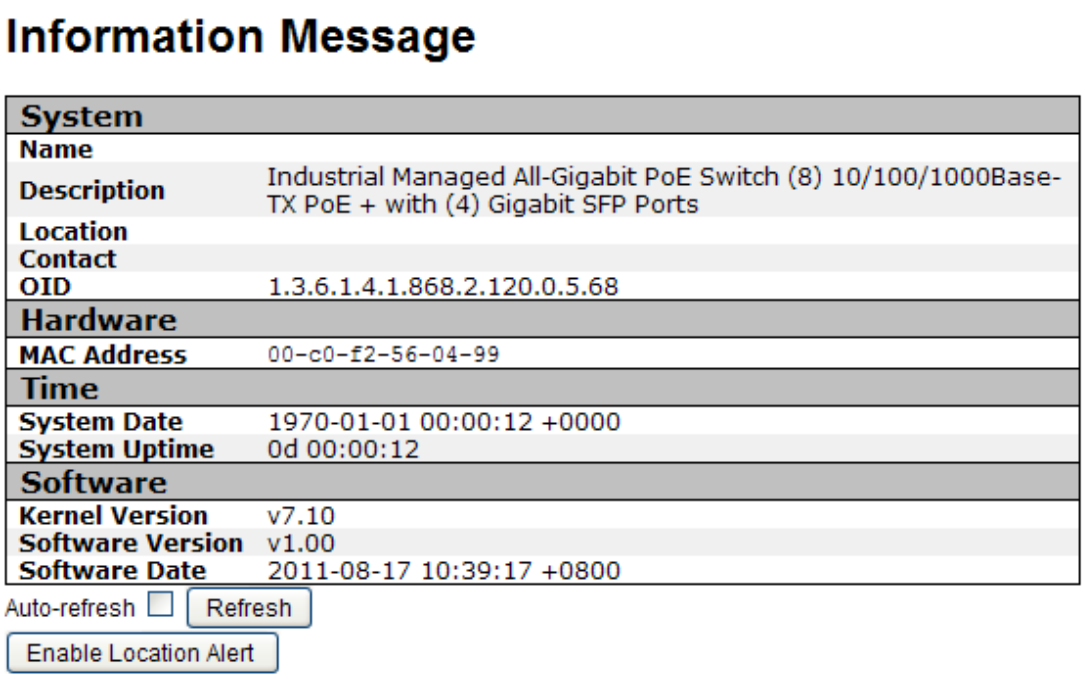
1. Launch the Internet Explorer.
2. Type http:// and the IP address of the switch. Press "**Enter**".



3. The login screen appears.
4. Key in the username and password. The default username and password is **"admin".**
5. Click "**Enter**" or"**OK**" button, then the main interface of the Web-based management appears.

Login screen

Main Interface

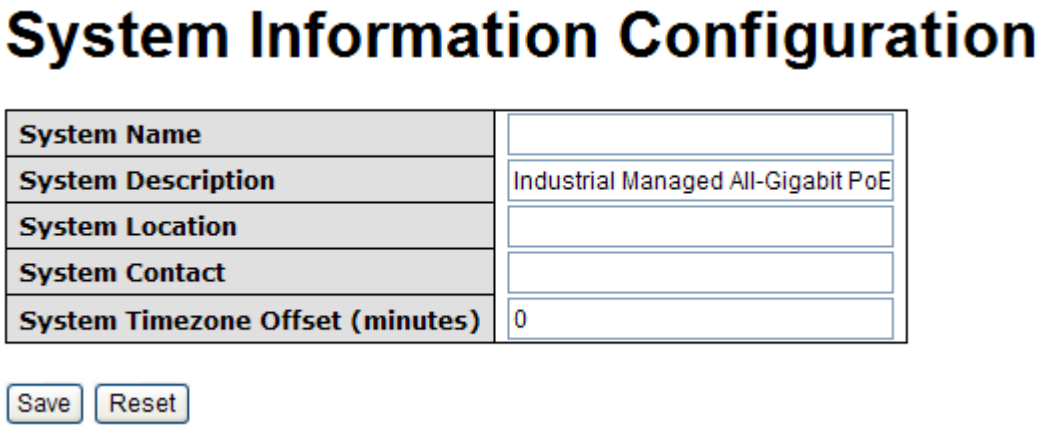


Main Interface

3.1.2 Basic Settings

3.1.2.1 System Information

The switch system information is provided here.



System Information interface

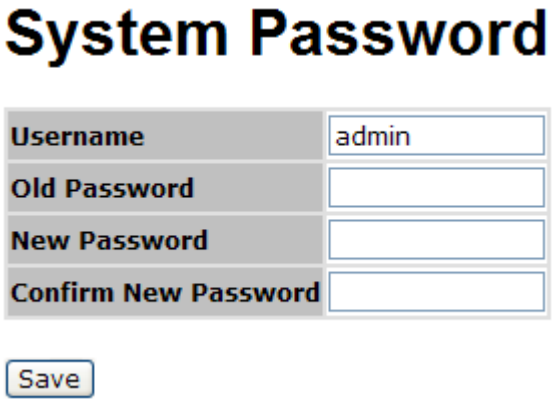
.

Label	Description
System Contact	The textual identification of the contact person for this managed

	node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
System Name	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Z, a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
System Location	The physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
Time zone Offset	Enter the name of contact person or organization Provide the time zone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

3.1.2.2 Admin & Password

This page allows you to configure the system password required to access the web pages or log in from CLI.

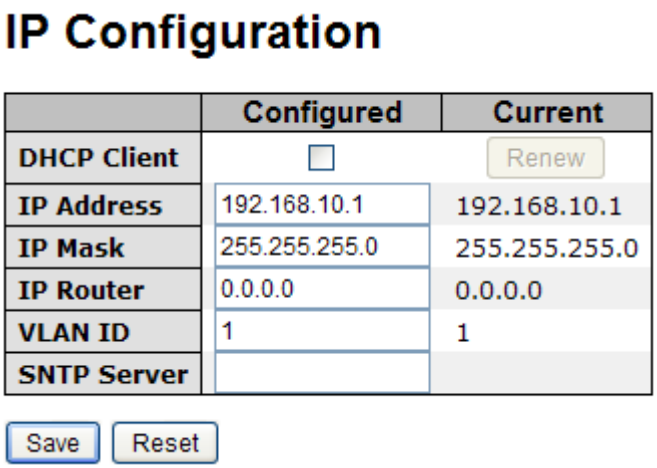


Label	Description

Old Password	Enter the current system password. If this is incorrect, the new password will not be set.
New Password	The system password. The allowed string length is 0 to 31, and the allowed content is the ASCII characters from 32 to 126.
Confirm password	Re-type the new password.
Save	Click to save changes.

3.1.2.3 IP Address Setting

Configure the switch-managed IP information on this page.



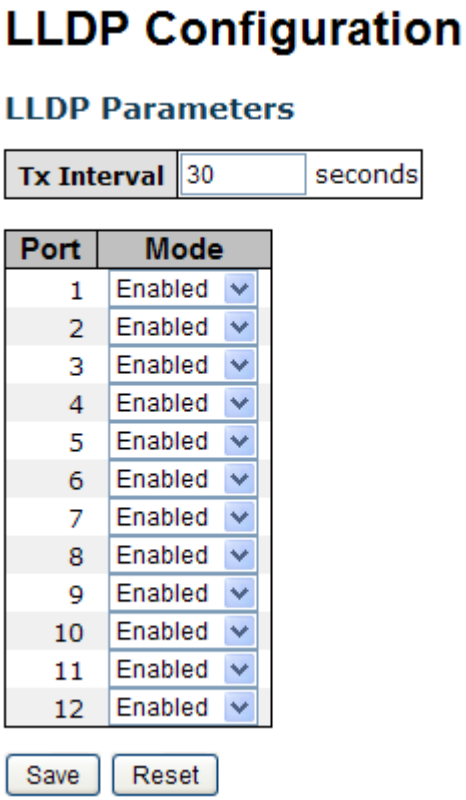
Label	Description
DHCP Client	Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

IP Address	Assign the IP address that the network is using. If DHCP client function is enabling, you do not need to assign the IP address. The network DHCP server will assign the IP address for the switch and it will be display in this column. The default IP is 192.168.10.1
IP Mask	Assign the subnet mask of the IP address. If DHCP client function is enabled, you do not need to assign the subnet mask
IP Router	Assign the network gateway for the switch. The default gateway is 192.168.10.254
VLAN ID	Provide the managed VLAN ID. The allowed range is 1 through 4095.
SNTP Server	SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Renew	Click to renew DHCP. This button is only available if DHCP is enabled.

3.1.2.4 LLDP

LLDP Parameters

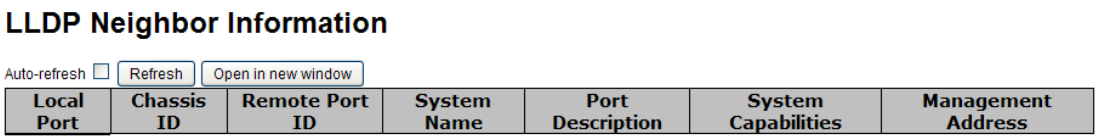
This page allows the user to inspect and configure the current LLDP port settings.



Label	Description
TX Interval	The switches will periodically transmit LLDP frames to its neighbors in order for the network discovery information to be up-to-date. The interval between each LLDP frame is determined by the TX Interval value. Valid values are restricted to 5 - 32768 seconds.

LLDP Neighbor Information

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The columns hold the following information:



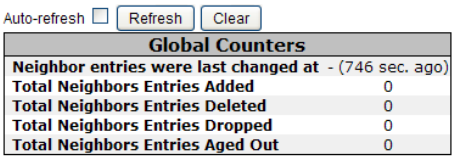
Label	Description

Local Port	The port on which the LLDP frame was received.
Chassis ID	The Chassis ID is the identification of the neighbor's LLDP frames.
Remote Port ID	The Remote Port ID is the identification of the neighbor port.
System Name	System Name is the name advertised by the neighbor unit.
Port Description	Port Description is the port description advertised by the neighbor unit.
System Capabilities	System Capabilities describes the neighbor unit's capabilities. The possible capabilities are: 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).
Management Address	Management Address is the neighbor unit's address that is used for higher layer entities to assist the discovery by the network management. This could for instance hold the neighbor's IP address.
Refresh	Click to refresh the page immediately.
Auto-refresh ☐	Check this box to enable an automatic refresh of the page at regular intervals.

LLDP Statistics

This page provides an overview of all LLDP traffic.

Two types of counters are shown. Global counters are counters that refer to the whole stack, switch, while local counters refer to counters for the currently selected switch.


Auto-refresh
Refresh
Clear
Global Counters
Neighbor entries were last changed at - (746 sec. ago)
Total Neighbors Entries Added 0
Total Neighbors Entries Deleted 0
Total Neighbors Entries Dropped 0
Total Neighbors Entries Aged Out 0

LLDP Statistics

Local Counters								
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	26	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0

Global Counters

Label	Description
Neighbor entries were last changed at	Shows the time for when the last entry was last deleted or added. It is also shows the time elapsed since last change was detected.
Total Neighbors Entries Added	Shows the number of new entries added since switch reboot.
Total Neighbors Entries Deleted	Shows the number of new entries deleted since switch reboot.
Total Neighbors Entries Dropped	Shows the number of LLDP frames dropped due to that the entry table was full.
Total Neighbors Entries Aged Out	Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

Label	Description
Local Port	The port on which LLDP frames are received or transmitted.
Tx Frames	The number of LLDP frames transmitted on the port.
Rx Frames	The number of LLDP frames received on the port.
Rx Errors	The number of received LLDP frames containing some kind of error.
Frames Discarded	If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port links

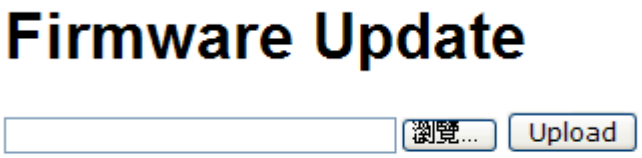
	down, an LLDP shutdown frame is received, or when the entry ages out.
TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
TLVs Unrecognized	The number of well-formed TLVs, but with an unknown type value.
Org. Discarded	The number of organizationally TLVs received.
Age-Outs	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.
Refresh	Click to refresh the page immediately.
Clear	Clears the local counters. All counters (including global counters) are cleared upon reboot.
Auto-refresh ☐	Check this box to enable an automatic refresh of the page at regular intervals.

3.1.2.5 Backup/Restore Configuration

You can save/view or load the switch configuration. The configuration file is in XML format with a hierarchy of tags:

3.1.2.6 Firmware Update

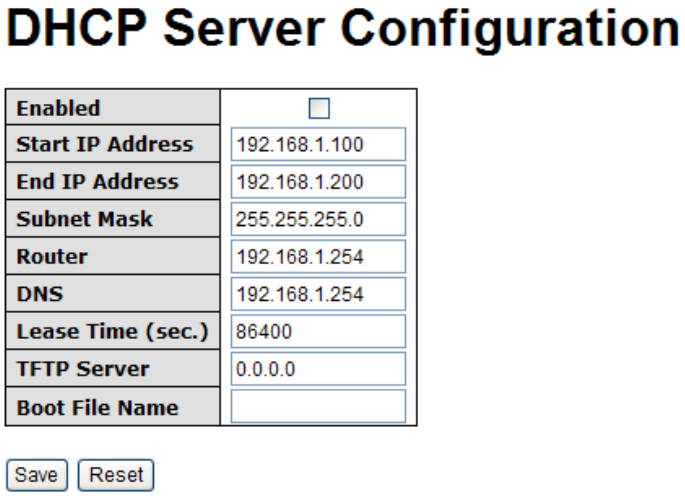
This page facilitates an update of the firmware controlling the stack. switch.



3.1.3 DHCP Server

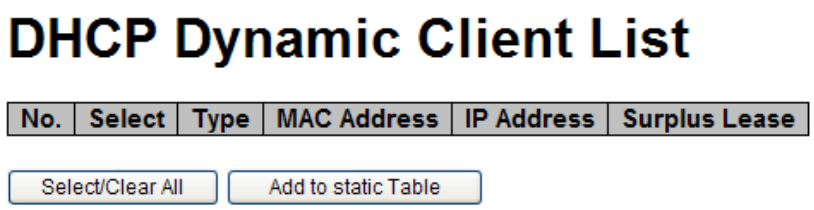
3.1.3.1 Setting

The system provides with DHCP server function. Enable the DHCP server function, the switch system will be a DHCP server.



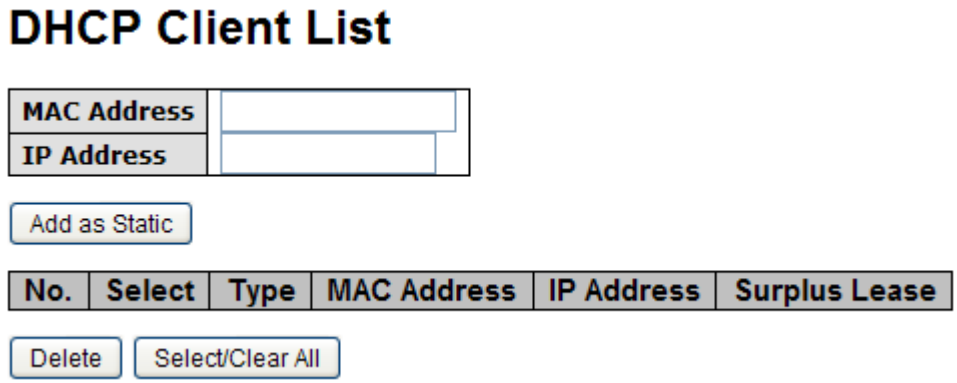
3.1.3.2 DHCP Dynamic Client List

When the DHCP server function is activated, the system will collect the DHCP client information and display in here.



3.1.3.3 DHCP Client List

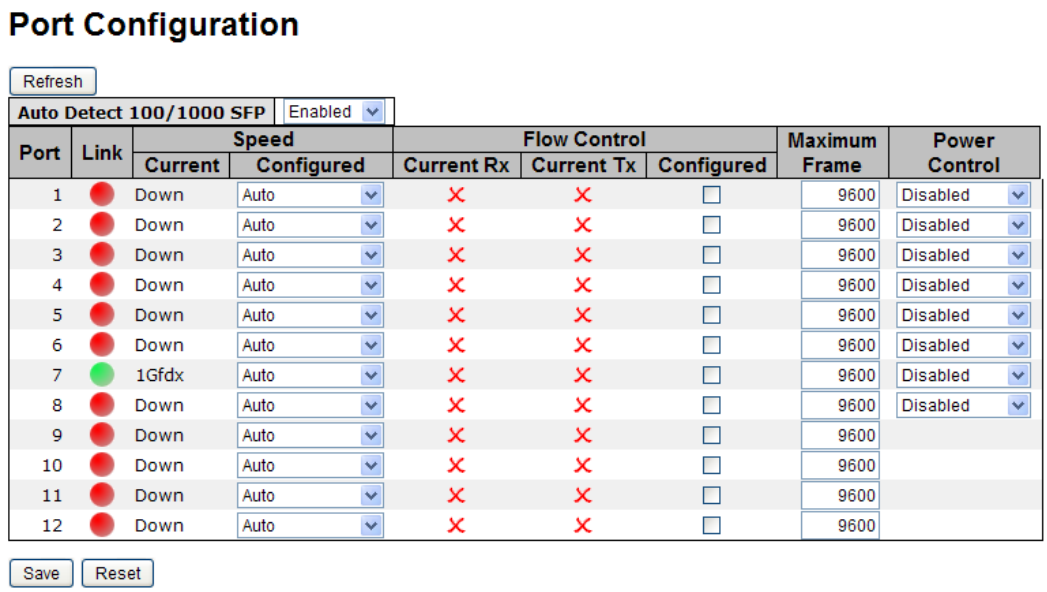
You can assign the specific IP address which is in the assigned dynamic IP range to the specific port. When the device is connecting to the port and asks for dynamic IP assigning, the system will assign the IP address that has been assigned before in the connected device.



3.1.4 Port Setting

3.1.4.1 Port Control

This page displays current port configurations. Ports can also be configured here.



Label	Description
Port	This is the logical port number for this row.
Link	The current link state is displayed graphically. Green indicates the link is up and red that it is down.
Current Link Speed	Provides the current link speed of the port.
Configured Link Speed	Select any available link speed for the given switch port. Auto Speed selects the highest speed that is compatible with a link partner. Disabled disables the switch port operation.
Flow Control	When Auto Speed is selected for a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current TX column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.
Maximum Frame	Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is 1518 bytes to 9600 bytes.
Excessive Collision Mode	Configure port transmit collision behavior. Discard: Discard frame after 16 collisions (default). Restart: Restart back off algorithm after 16 collisions.
Power Control	The Usage column shows the current percentage of the power consumption per port. The Configured column allows for changing the power savings mode parameters per port. Disabled: All power savings mechanisms disabled. ActiPHY: Link down power savings enabled. PerfectReach: Link up power savings enabled. Enabled: Both link up and link down power savings enabled.
Total Power Usage	Total power usage in board, measured in percent.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Refresh	Click to refresh the page. Any changes made locally will be undone.

3.1.4.2 Rate Limit

Configure the switch port rate limit for Policers and Shapers on this page.

Rate Limit Configuration

Port	Policer Enabled	Policer Rate	Policer Unit	Shaper Enabled	Shaper Rate	Shaper Unit
1	☐	500	kbps	☐	500	kbps
2	☐	500	kbps	☐	500	kbps
3	☐	500	kbps	☐	500	kbps
4	☐	500	kbps	☐	500	kbps
5	☐	500	kbps	☐	500	kbps
6	☐	500	kbps	☐	500	kbps
7	☐	500	kbps	☐	500	kbps
8	☐	500	kbps	☐	500	kbps
9	☐	500	kbps	☐	500	kbps
10	☐	500	kbps	☐	500	kbps
11	☐	500	kbps	☐	500	kbps
12	☐	500	kbps	☐	500	kbps

Save Reset

Label	Description
Port	The logical port for the settings contained in the same row.
Policer Enabled	Enable or disable the port policer. The default value is "Disabled".
Policer Rate	Configure the rate for the port policer. The default value is "500". This value is restricted to 500-1000000 when the "Policer Unit" is "kbps", and it is restricted to 1-1000 when the "Policer Unit" is "Mbps"
Policer Unit	Configure the unit of measure for the port policer rate as kbps or Mbps. The default value is "kbps".
Shaper Enabled	Enable or disable the port shaper. The default value is "Disabled".
Shaper Rate	Configure the rate for the port shaper. The default value is "500". This value is restricted to 500-1000000 when the "Policer Unit" is

	"kbps", and it is restricted to 1-1000 when the "Policer Unit" is "Mbps"
Shaper Unit	Configure the unit of measure for the port shaper rate as kbps or Mbps. The default value is "kbps".
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

3.1.4.3 Port Trunk

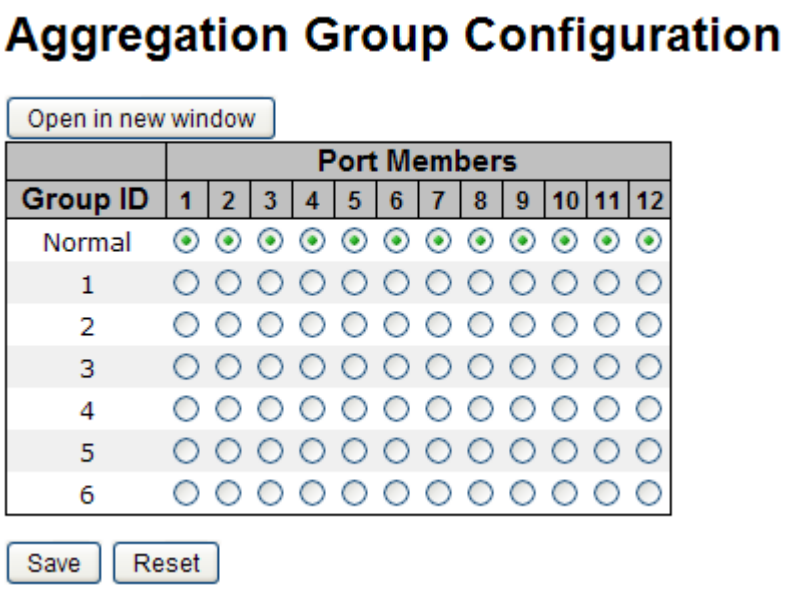
3.1.4.3.1 Trunk Configuration

This page is used to configure the Aggregation hash mode and the aggregation group.

Aggregation Mode Configuration

Hash Code Contributors	
Source MAC Address	☑
Destination MAC Address	☐
IP Address	☑
TCP/UDP Port Number	☑

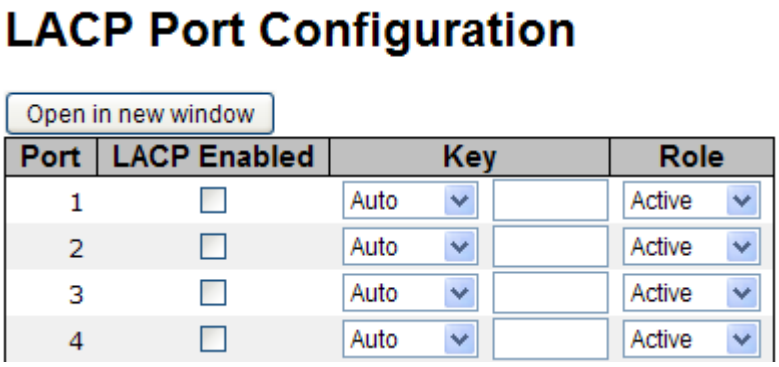
Label	Description
Source MAC Address	The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.
Destination MAC Address	The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.
IP Address	The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.
TCP/UDP Port Number	The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.



Label	Description
Group ID	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
Port Members	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

3.1.4.3.2 LACP Port Configuration

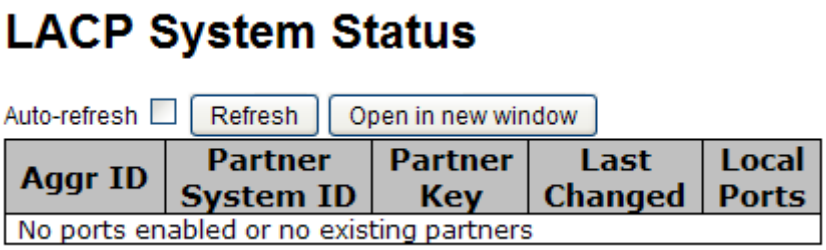
This page allows the user to inspect the current LACP port configurations, and possibly change them as well.



Label	Description
Port	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
LACP Enabled	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.
Key	The Key value incurred by the port, range 1-65535. The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.
Role	The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

3.1.4.3.3 LACP System Status

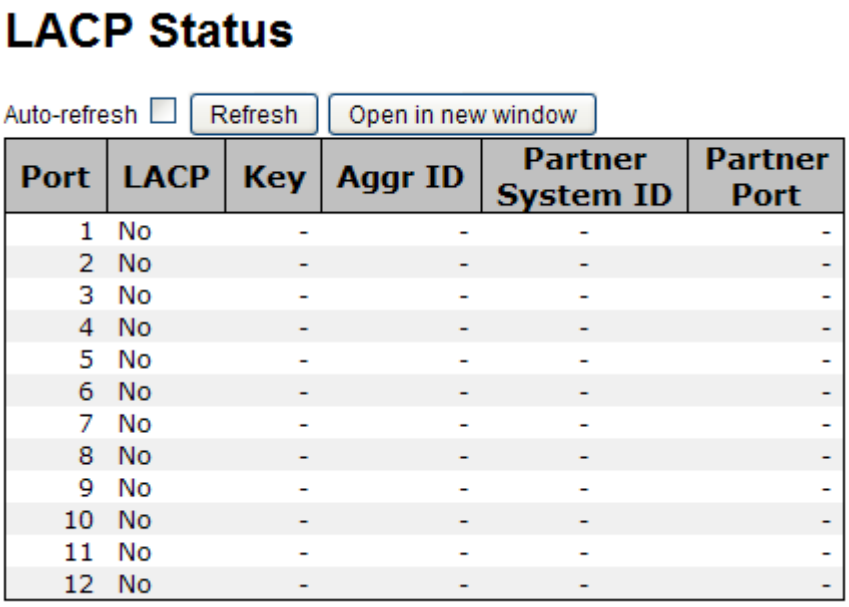
This page provides a status overview for all LACP instances.



Label	Description
Aggr ID	The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'
Partner System ID	The system ID (MAC address) of the aggregation partner.
Partner Key	The Key that the partner has assigned to this aggregation ID.
Last Changed	The time since this aggregation changed.
Last Changed	Shows which ports are a part of this aggregation for this switch/stack. The format is: "Switch ID: Port".
Refresh	Click to refresh the page immediately.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.

3.1.4.3.4 LACP Status

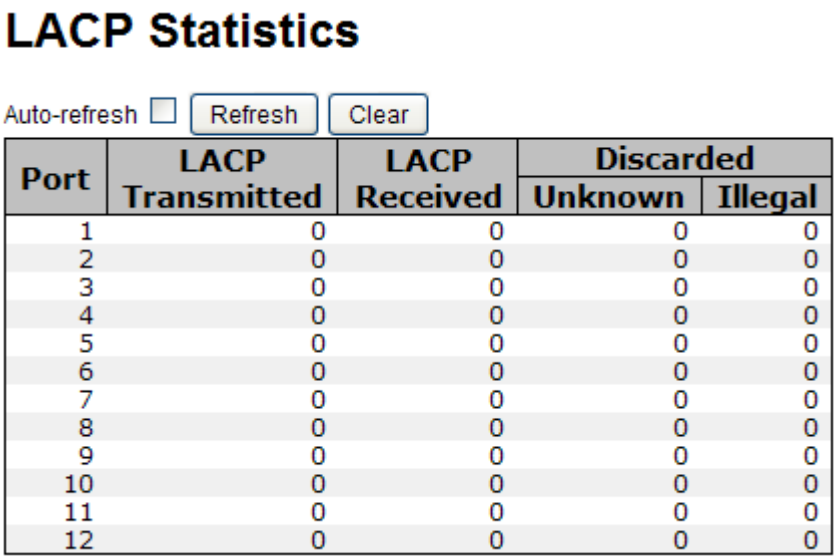
This page provides a status overview for LACP status for all ports.


LACP Status
Auto-refresh
Refresh
Open in new window
Port LACP Key Aggr ID Partner System ID Partner Port
1 No - - - -
2 No - - - -
3 No - - - -
4 No - - - -
5 No - - - -
6 No - - - -
7 No - - - -
8 No - - - -
9 No - - - -
10 No - - - -
11 No - - - -
12 No - - - -

Label	Description
Port	The switch port number.
LACP	'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.
Key	The key assigned to this port. Only ports with the same key can aggregate together.
Aggr ID	The Aggregation ID assigned to this aggregation group.
Partner System ID	The partners System ID (MAC address).
Partner Port	The partners port number connected to this port.
Refresh	Click to refresh the page immediately.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.

3.1.4.3.5 LACP Statistics

This page provides an overview for LACP statistics for all ports.

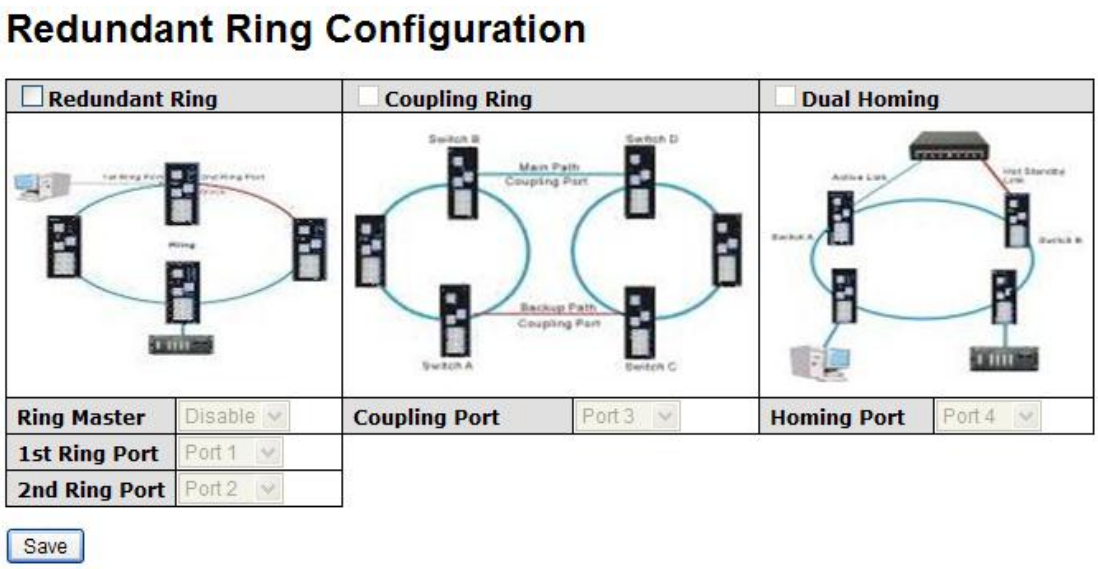


Label	Description
Port	The switch port number
LACP Transmitted	Shows how many LACP frames have been sent from each port
LACP Received	Shows how many LACP frames have been received at each port.
Discarded	Shows how many unknown or illegal LACP frames have been discarded at each port.
Refresh	Click to refresh the page immediately.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Clear	Clears the counters for all ports

3.1.5 Redundancy

3.1.5.1 Redundant Ring.

ERing is the most powerful Ring technology in the world. The recovery time of eRing is less than 10 ms. It can reduce unexpected damage caused by network topology changes. ERing Supports 3 Ring topologies: Ring, Coupling Ring and Dual Homing.



Ring interface

The following table describes the labels in this screen.

Label	Description
Redundant Ring	Mark to enable Ring.
Ring Master	There should be one and only one Ring Master in a ring. However if there are two or more switches which set Ring Master to enable, the switch with the lowest MAC address will be the actual Ring Master and others will be Backup Masters.
1st Ring Port	The primary port, when this switch is Ring Master.
2nd Ring Port	The backup port, when this switch is Ring Master.
Coupling Ring	Mark to enable Coupling Ring. Coupling Ring can be used to divide a big ring into two smaller rings to avoid effecting all switches when network topology change. It is a good application for connecting two Rings.
Coupling Port	Link to Coupling Port of the switch in another ring. Coupling Ring need four switch to build an active and a backup link. Set a port as coupling port. The coupled four ports of four switches will be run at active/backup mode.
Dual Homing	Mark to enable Dual Homing. By selecting Dual Homing mode, Ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work as active/backup mode, and connect each Ring to the normal switches in RSTP mode.
Apply	Click "**Apply**" to set the configurations.

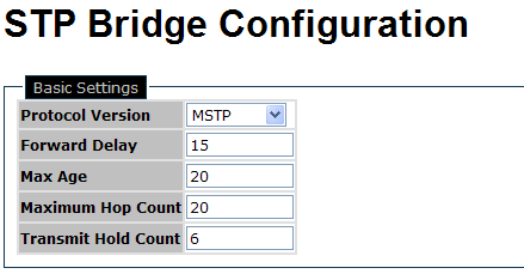
Note: We don't suggest you to set one switch as a Ring Master and a Coupling Ring at the

same time due to heavy load.

3.1.5.2 MSTP

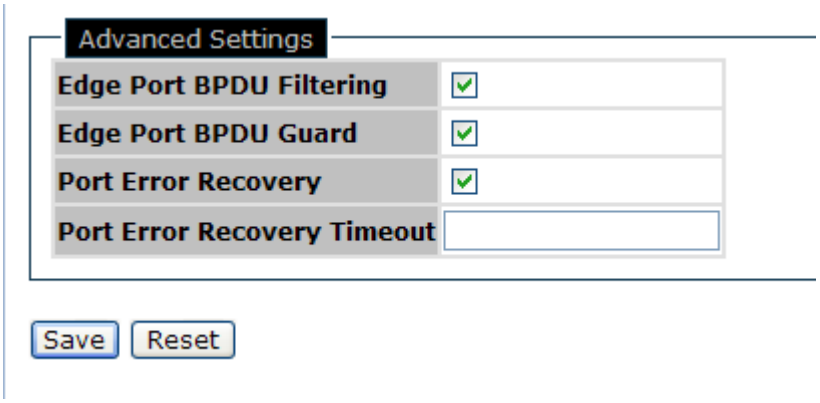
Bridge Settings

This page allows you to configure RSTP system settings. The settings are used by all RSTP Bridge instances in the Switch Stack.



Label	Description
Protocol Version	The STP protocol version setting. Valid values are STP, RSTP and MSTP.
Forward Delay	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.
Max Age	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.
Maximum Hop Count	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information. Valid values are in the range 4 to 30 seconds, and MaxAge must be <= (FwdDelay-1)*2.
Transmit Hold Count	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

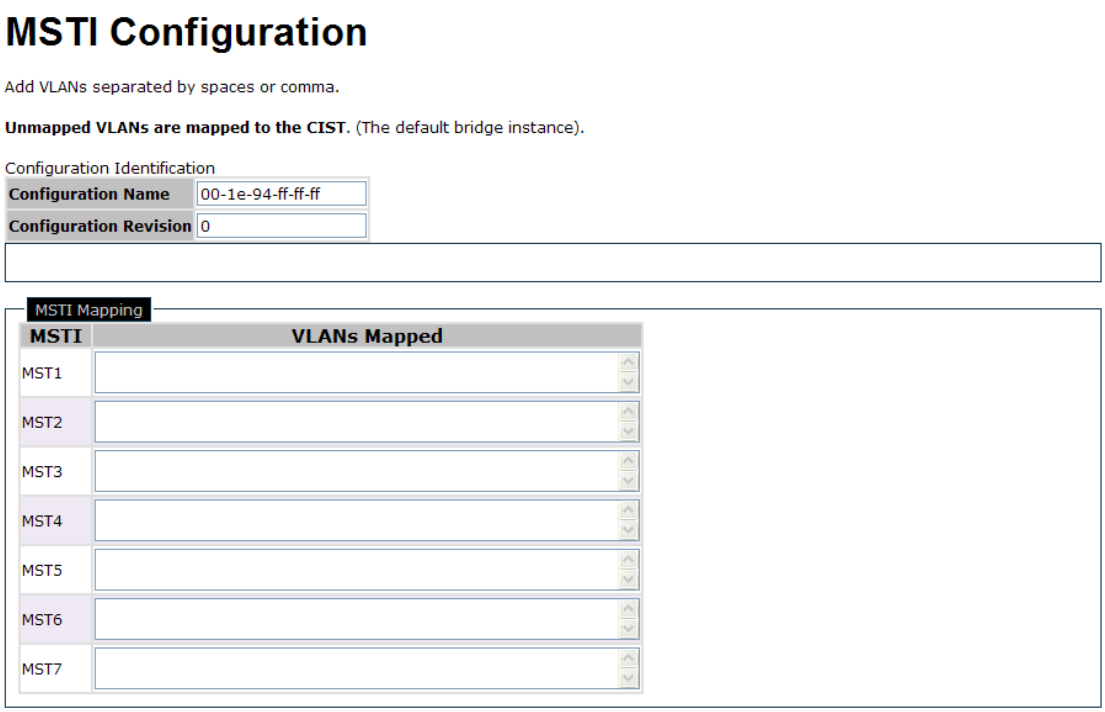
Advanced Settings



Label	Description
Edge Port BPDU Filtering	Control whether a port explicitly configured as Edge will transmit and receive BPDUs.
Edge Port BPDU Guard	Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.
Port Error Recovery	Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.
Port Error Recovery Timeout	The time that has to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

MSTI Mapping

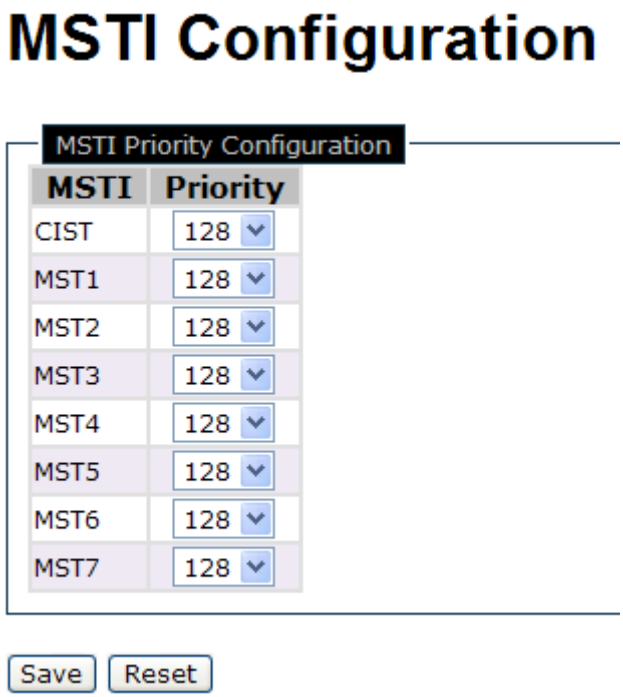
This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.



Label	Description
Configuration Name	The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's. (Intra-region). The name is at most 32 characters.
Configuration Revision	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.
MSTI	The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.
VLANS Mapped	The list of VLAN's mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. A unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.)
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

MSTI Priorities

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

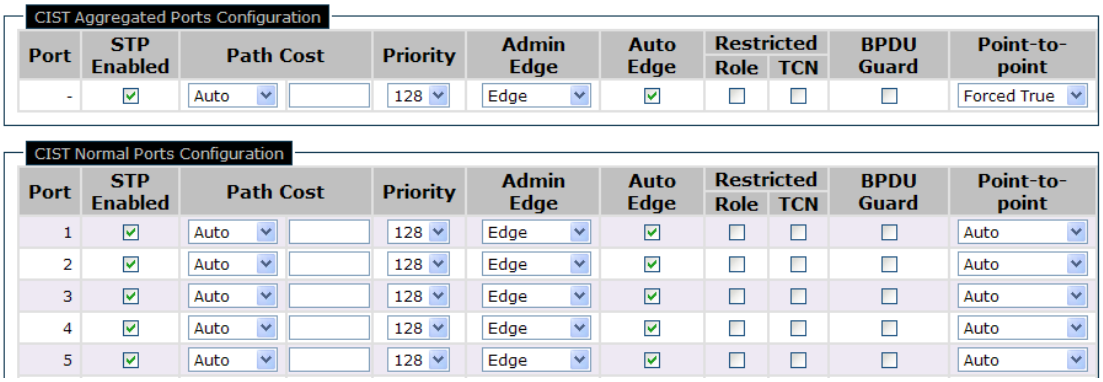


Label	Description
MSTI	The bridge instance. The CIST is the default instance, which is always active.
Priority	Controls the bridge priority. Lower numerical values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

CIST Ports

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well. This page contains settings for physical and aggregated ports. The aggregation settings are stack global.

STP CIST Ports Configuration



CIST Aggregated Ports Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted Role	Restricted TCN	BPDU Guard	Point-to-point
-	☑	Auto		128	Edge	☑	☐	☐	☐	Forced True

CIST Normal Ports Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted Role	Restricted TCN	BPDU Guard	Point-to-point
1	☑	Auto		128	Edge	☑	☐	☐	☐	Auto
2	☑	Auto		128	Edge	☑	☐	☐	☐	Auto
3	☑	Auto		128	Edge	☑	☐	☐	☐	Auto
4	☑	Auto		128	Edge	☑	☐	☐	☐	Auto
5	☑	Auto		128	Edge	☑	☐	☐	☐	Auto

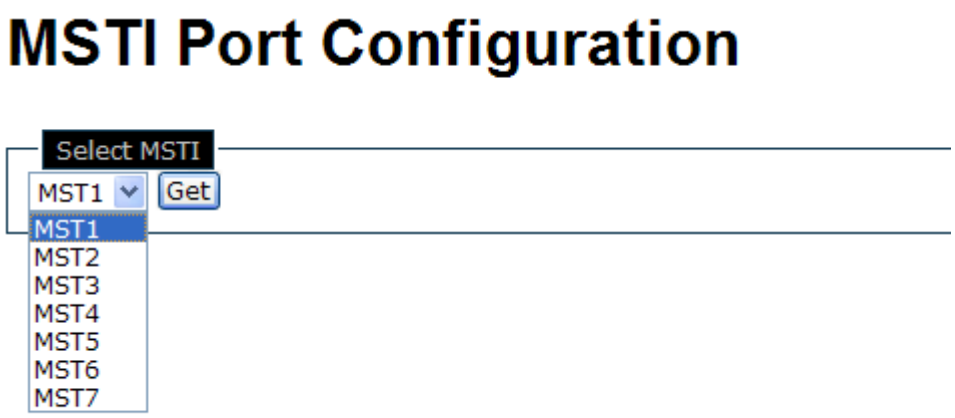
Label	Description
Port	The switch port number of the logical STP port.
STP Enabled	Controls whether STP is enabled on this switch port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
OpenEdge (set the flag)	Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transitioning to the forwarding state is faster for edge ports (having OpenEdge true) than for other ports.
AdminEdge	Controls whether the OpenEdge flag should start as being set or cleared. (The initial OpenEdge state when a port is initialized).
AutoEdge	Controls whether the bridge should enable automatic edge detection on the bridge port. This allows OpenEdge to be derived from whether BPDU's are received on the port or not.
Restricted Role	If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to

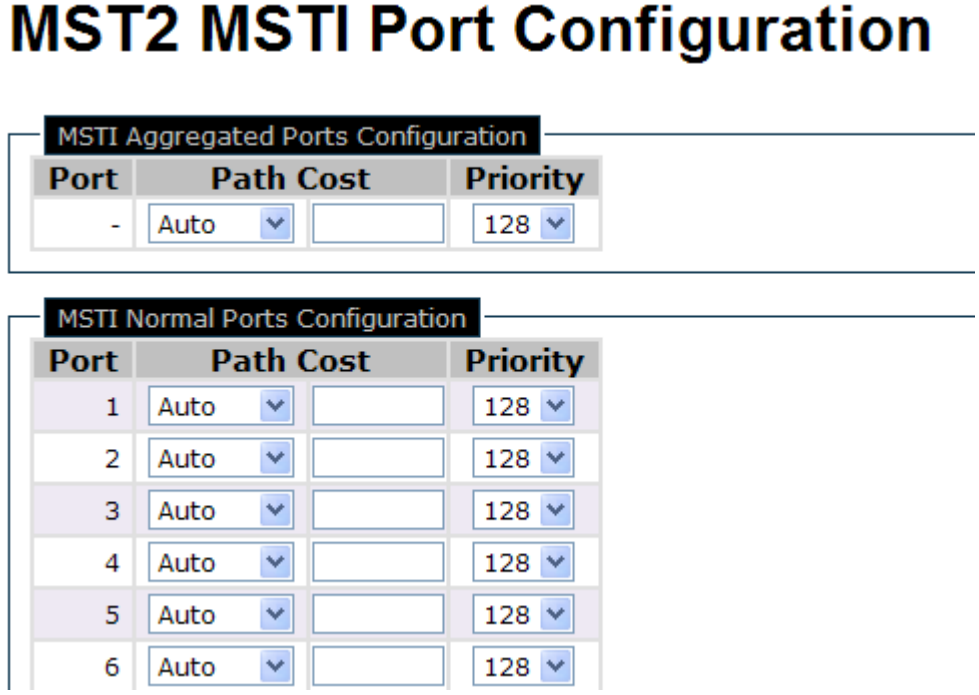
	prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also know as Root Guard.
Restricted TCN	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning trees active topology as a result of persistent incorrectly learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or is the physical link state for the attached LANs transitions frequently.
Point2Point	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

MSTI Ports

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well. A MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured and applicable for the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

This page contains MSTI port settings for physical and aggregated ports. The aggregation settings are stack global.





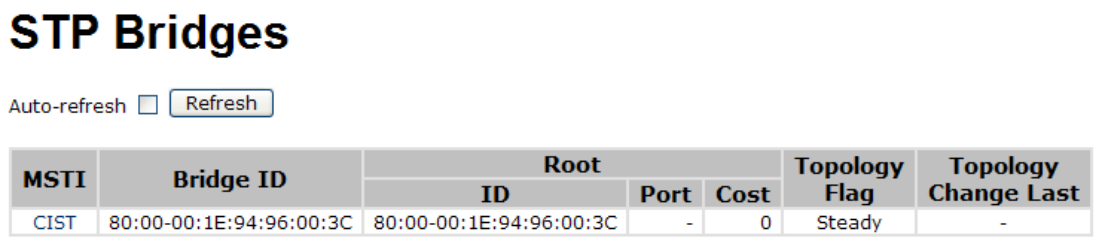
Label	Description
Port	The switch port number of the corresponding STP CIST (and MSTI) port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of

	ports having identical port cost. (See above).
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

STP Bridges

This page provides a status overview for all STP bridge instances.

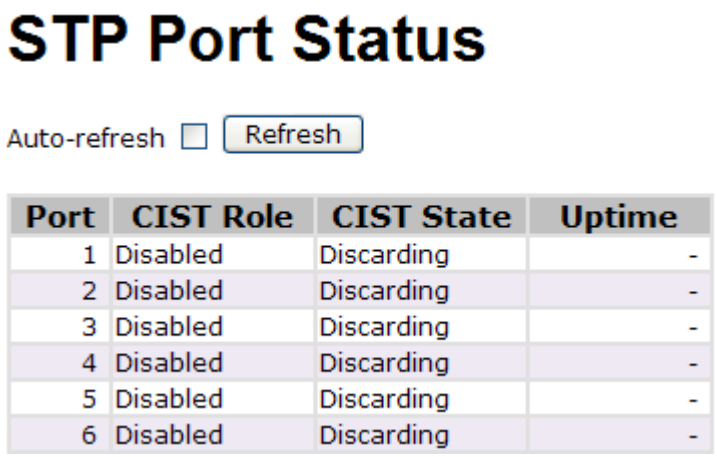
The displayed table contains a row for each STP bridge instance, where the column displays the following information:



Label	Description
MSTI	The Bridge Instance. This is also a link to the STP Detailed Bridge Status.
Bridge ID	The Bridge ID of this Bridge instance.
Root ID	The Bridge ID of the currently elected root bridge.
Root Port	The switch port currently assigned the root port role.
Root Cost	Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
Topology Flag	The current state of the Topology Change Flag for this Bridge instance.
Topology Change Last	The time since last Topology Change occurred.
Refresh	Click to refresh the page immediately.
Auto-refresh ☐	Check this box to enable an automatic refresh of the page at regular intervals.

STP Port Status

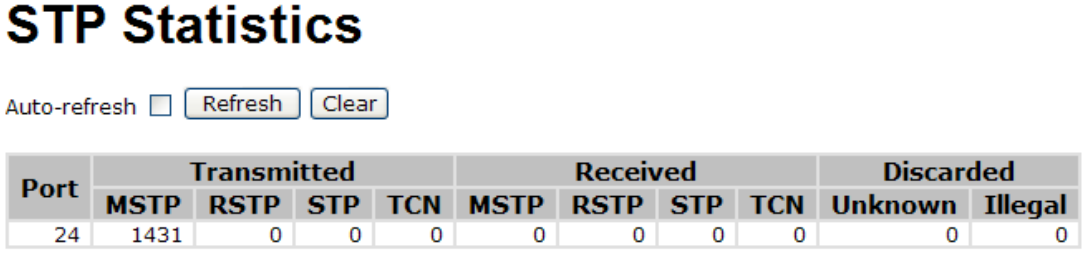
This page displays the STP CIST port status for port physical ports in the currently selected switch.

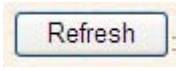
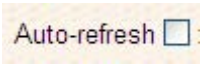


Label	Description
Port	The switch port number of the logical STP port.
CIST Role	The current STP port role of the CIST port. The port role can be one of the following values: Alternate Port, Backup Port, Root Port & Designated Port.
State	The current STP port state of the CIST port. The port state can be one of the following values: Blocking Learning Forwarding.
Uptime	The time since the bridge port was last initialized.
Refresh	Click to refresh the page immediately.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.

STP Statistics

This page displays the RSTP port statistics counters for bridge ports in the currently selected switch.

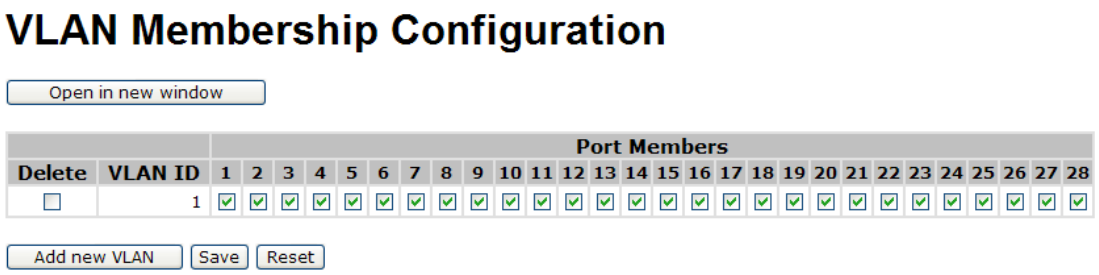

STP Statistics
Auto-refresh
Refresh
Clear
Port Transmitted Received Discarded
MSTP RSTP STP TCN MSTP RSTP STP TCN Unknown Illegal
24 1431 0 0 0 0 0 0 0 0 0

Label	Description
Port	The switch port number of the logical RSTP port.
RSTP	The number of RSTP Configuration BPDU's received/transmitted on the port.
STP	The number of legacy STP Configuration BPDU's received/transmitted on the port.
TCN	The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.
Discarded Unknown	The number of unknown Spanning Tree BPDU's received (and discarded) on the port.
Discarded Illegal	The number of illegal Spanning Tree BPDU's received (and discarded) on the port.
	Click to refresh the page immediately.
	Check this box to enable an automatic refresh of the page at regular intervals.

3.1.6 VLAN

3.1.6.1 VLAN Membership Configuration

The VLAN membership configuration for the selected stack switch unit switch can be monitored and modified here. Up to 64 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.

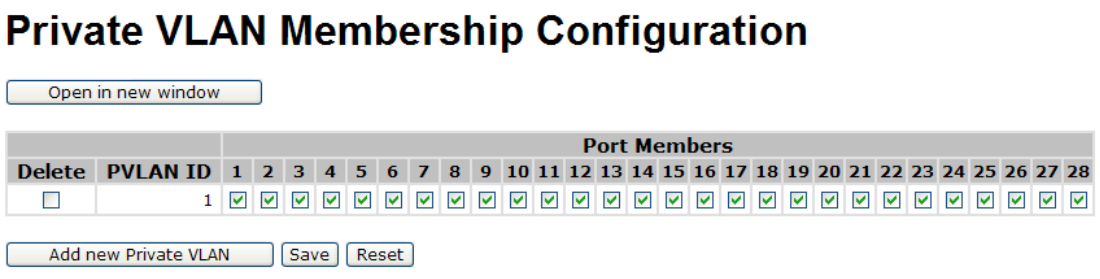

VLAN Membership Configuration
Open in new window
Port Members
Delete
VLAN ID
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
1
Add new VLAN
Save
Reset

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
MAC Address	The MAC address for the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Adding a New Static Entry	Click Add New VLAN to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The VLAN is enabled on the selected stack switch unit when you click on "Save". The VLAN is thereafter present on the other stack switch units, but with no port members. A VLAN without any port members on any stack unit will be deleted when you click "Save". The Delete button can be used to undo the addition of new VLANs.

3.1.6.2 Private VLAN

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical. A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.
A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.


Private VLAN Membership Configuration
Open in new window
Port Members
Delete
PVLAN ID
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
1
Add new Private VLAN
Save
Reset

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Private VLAN ID	Indicates the ID of this particular private VLAN.
MAC Address	The MAC address for the entry.
Port Members	A row of check boxes for each port is displayed for each private

	VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Adding a New Static Entry	Click Add New Private VLAN to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction. The Private VLAN is enabled when you click "Save". The Delete button can be used to undo the addition of new Private VLANs.

Port Isolation Configuration

Open in new window

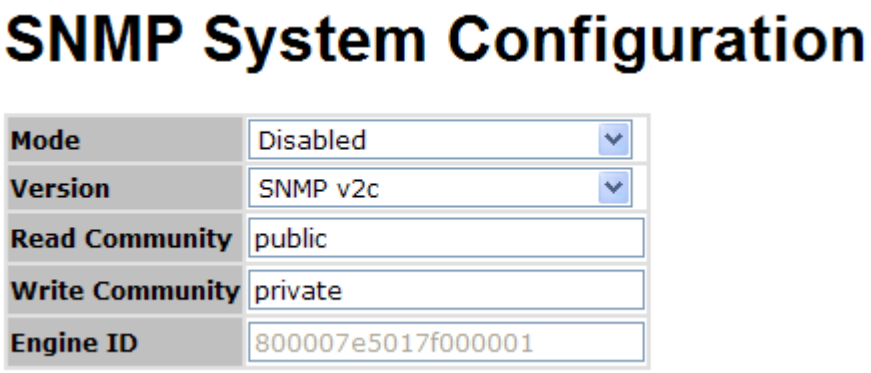
Port Number																									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Save Reset

Label	Description
Port Members	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled for that port. When unchecked, port isolation is disabled for that port. By default, port isolation is disabled for all ports.

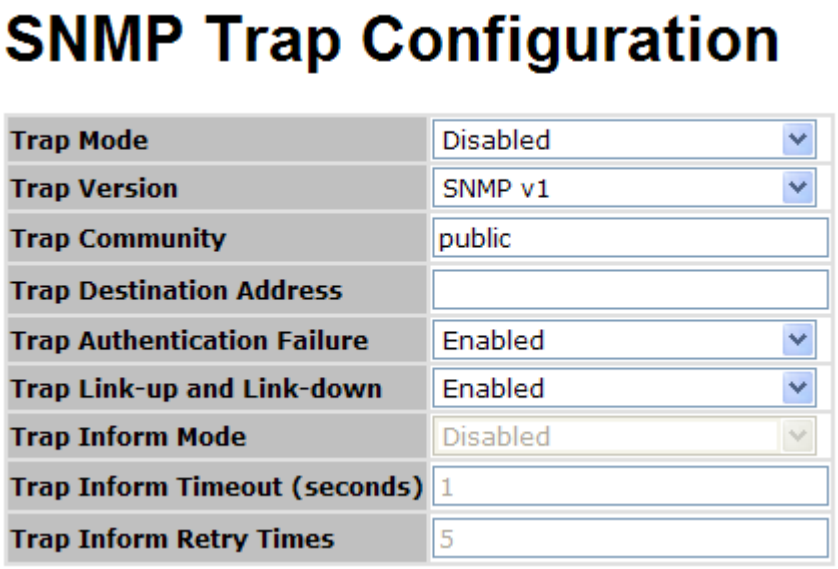
3.1.7 SNMP

3.1.7.1 SNMP-System



Label	Description
Mode	Indicates the SNMP mode operation. Possible modes are: Enabled: Enable SNMP mode operation. Disabled: Disable SNMP mode operation.
Version	Indicates the SNMP supported version. Possible versions are: SNMP v1: Set SNMP supported version 1. SNMP v2c: Set SNMP supported version 2c. SNMP v3: Set SNMP supported version 3.
Read Community	Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field only suits to SNMPv1 and SNMPv2c. SNMPv3 is using

	USM for authentication and privacy and the community string will associated with SNMPv3 communities table
Write Community	Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field only suits to SNMPv1 and SNMPv2c. SNMPv3 is using USM for authentication and privacy and the community string will associated with SNMPv3 communities table.
Engine ID	Indicates the SNMPv3 engine ID. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.



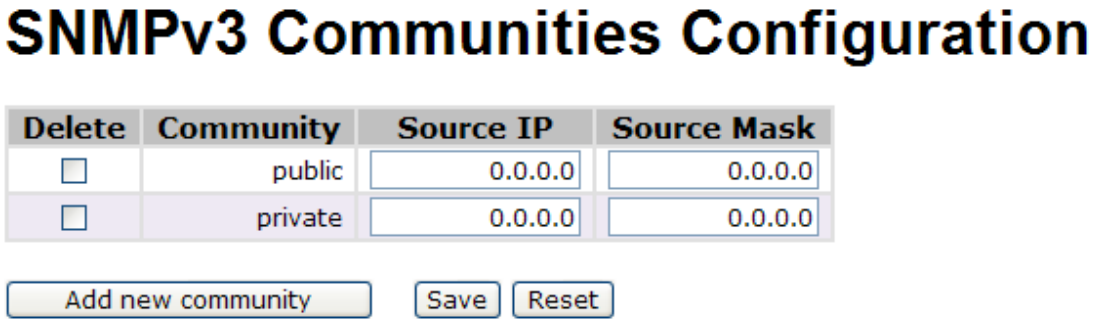
Label	Description
Trap Mode	Indicates the SNMP trap mode operation. Possible modes are: Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation.
Trap Version	Indicates the SNMP trap supported version. Possible versions are: SNMP v1: Set SNMP trap supported version 1. SNMP v2c: Set SNMP trap supported version 2c. SNMP v3: Set SNMP trap supported version 3.
Trap Community	Indicates the community access string when send SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.

Trap Destination Address	Indicates the SNMP trap destination address. Trap Destination IPv6 Address
Trap Destination IPv6 Address	Provide the trap destination IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separate each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example, '::192.1.2.34'.
Trap Authentication Failure	Indicates the SNMP entity is permitted to generate authentication failure traps. Possible modes are: Enabled: Enable SNMP trap authentication failure. Disabled: Disable SNMP trap authentication failure.
Trap Link-up and Link-down	Indicates the SNMP trap link-up and link-down mode operation. Possible modes are: Enabled: Enable SNMP trap link-up and link-down mode operation. Disabled: Disable SNMP trap link-up and link-down mode operation.
Trap Inform Mode	Indicates the SNMP trap inform mode operation. Possible modes are: Enabled: Enable SNMP trap inform mode operation. Disabled: Disable SNMP trap inform mode operation.
Trap Inform Timeout(seconds)	Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.
Trap Inform Retry Times	Indicates the SNMP trap informs retry times. The allowed range is 0 to 255.
Trap Probe Security Engine ID	Indicates the SNMP trap probe security engine ID mode of operation. Possible values are: Enabled: Enable SNMP trap probe security engine ID mode of operation. Disabled: Disable SNMP trap probe security engine ID mode of operation.
Trap Security Engine ID	Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number between 10 and 64 hexadecimal digits, but

	all-zeros and all-'F's are not allowed.
Trap Security Name	Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

3.1.7.2 SNMP-Communities

Configure SNMPv3 communities table on this page. The entry index key is Community.



Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Community	Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Source IP	Indicates the SNMP access source address.
Source Mask	Indicates the SNMP access source address mask.

3.1.7.3 SNMP-Users

Configure SNMPv3 users table on this page. The entry index keys are Engine ID and User Name.

SNMPv3 Users Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
☐	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

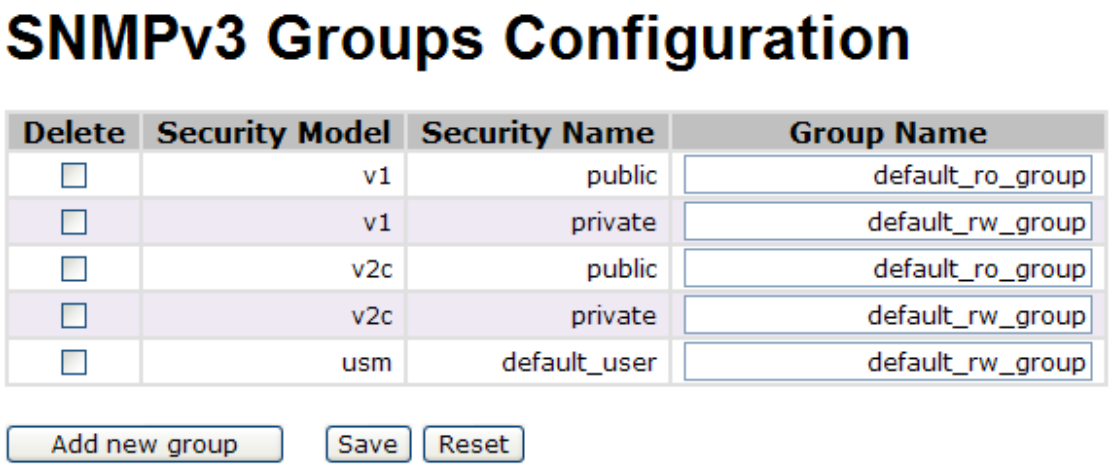
Add new user Save Reset

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In othe words, if user engine ID equal system engine ID then it is local user; otherwize it's remote user.
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Security Level	Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv: None authentication and none privacy. Auth, NoPriv: Authentication and none privacy. Auth, Priv: Authentication and privacy. The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
Authentication Protocol	Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are: None: None authentication protocol. MD5: An optional flag to indicate that this user using MD5 authentication protocol. SHA: An optional flag to indicate that this user using SHA authentication protocol.

	The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
Authentication Password	A string identifying the authentication pass phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is the ASCII characters from 33 to 126.
Privacy Protocol	Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are: None: None privacy protocol. DES: An optional flag to indicate that this user using DES authentication protocol.
Privacy Password	A string identifying the privacy pass phrase. The allowed string length is 8 to 32, and the allowed content is the ASCII characters from 33 to 126.

3.1.7.4 SNMP-Groups

Configure SNMPv3 groups table on this page. The entry index keys are Security Model and Security Name.



Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: v1: Reserved for SNMPv1. v2c: Reserved for SNMPv2c.

	usm: User-based Security Model (USM).
Security Name	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

3.1.7.5 SNMP-Views

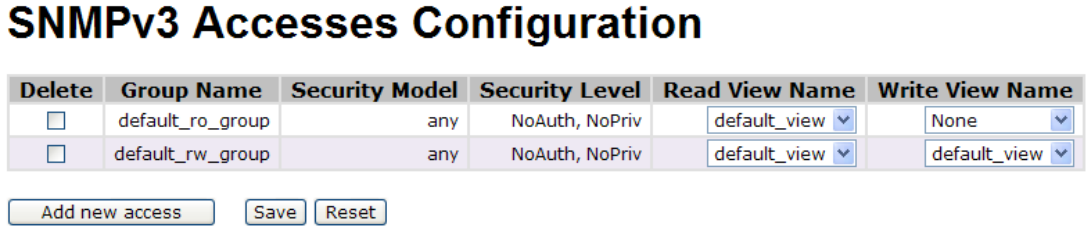
Configure SNMPv3 views table on this page. The entry index keys are View Name and OID Sub tree.

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
View Type	Indicates the view type that this entry should belong to. Possible view types are: Included: An optional flag to indicate that this view sub tree should be included. Excluded: An optional flag to indicate that this view sub tree should be excluded. General, if a view entry's view type is 'excluded', it should be exist another view entry which view type is 'included' and it's OID sub tree overstep the 'excluded' view entry.

OID Sub tree	The OID defining the root of the sub tree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk (*).

3.1.7.6 SNMP-Accesses

Configure SNMPv3 accesses table on this page. The entry index keys are Group Name, Security Model and Security Level.



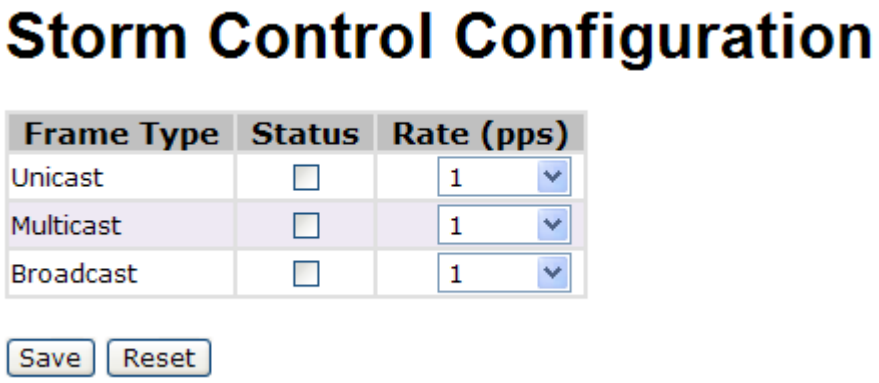
Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: any: Accepted any security model (v1|v2c|usm). v1: Reserved for SNMPv1. v2c: Reserved for SNMPv2c. usm: User-based Security Model (USM).
Security Level	Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv: None authentication and none privacy. Auth, NoPriv: Authentication and none privacy. Auth, Priv: Authentication and privacy.
Read View Name	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Write View Name	The name of the MIB view defining the MIB objects for which this request may potentially SET new values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to

	126.

3.1.8 Traffic Prioritization

3.1.8.1 Storm Control

Storm control for the switch is configured on this page.



There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

The rate is 2^n, where n is equal to or less than 15, or "No Limit". The unit of the rate can be either pps (packets per second) or kpps (kilopackets per second). The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch.

(Note: Frames, which are sent to the CPU of the switch, are always limited to approximately 4 kpps. For example, broadcasts in the management VLAN are limited to this rate. The management VLAN is configured on the IP setup page.)

Label	Description
Frame Type	The settings in a particular row apply to the frame type listed here: unicast, multicast, or broadcast.
Status	Enable or disable the storm control status for the given frame type.
Rate	The rate unit is packet per second (pps), configure the rate as 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K. The 1 kpps is actually 1002.1 pps.

3.1.8.2 Port Configuration

This page allows you to configure QoS settings for each port.

Frames can be classified by 4 different QoS classes: Low, Normal, Medium, and High.

The classification is controlled by a QCL that is assigned to each port.

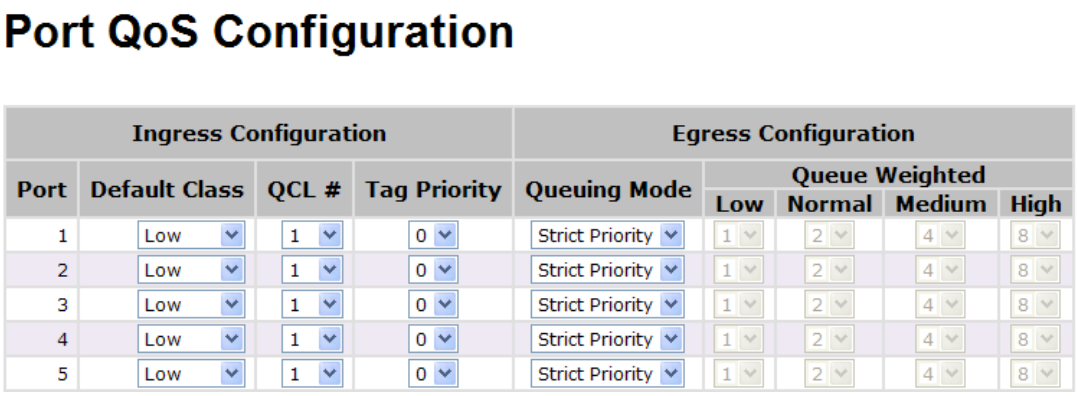
A QCL consists of an ordered list of up to 12 QCEs.

Each QCE can be used to classify certain frames to a specific QoS class.

This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 DSCP or Tag Priority.

Frames not matching any of the QCEs are classified to the default QoS class for the port.

Port Qos Configuration


Port QoS Configuration
Ingress Configuration
Egress Configuration
Port
Default Class
QCL #
Tag Priority
Queuing Mode
Queue Weighted
Low
Normal
Medium
High
1 Low 1 0 Strict Priority 1 2 4 8
2 Low 1 0 Strict Priority 1 2 4 8
3 Low 1 0 Strict Priority 1 2 4 8
4 Low 1 0 Strict Priority 1 2 4 8
5 Low 1 0 Strict Priority 1 2 4 8

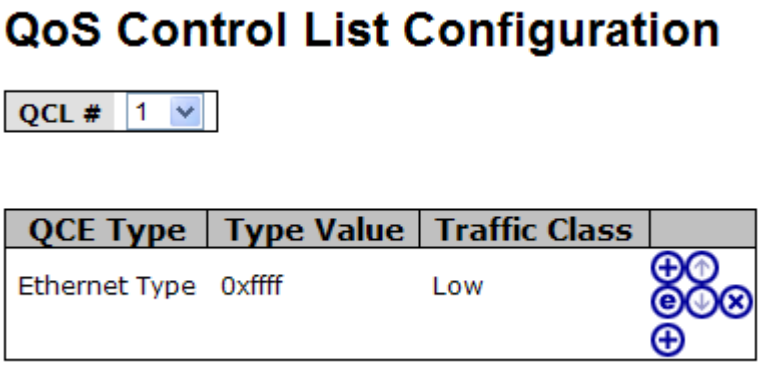
Label	Description
Port	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled for that port. When unchecked, port isolation is disabled for that port. By default, port isolation is disabled for all ports.
Default Class	Configure the default QoS class for the port, that is, the QoS class for frames not matching any of the QCEs in the QCL.
QCL#	Select which QCL to use for the port.
Tag Priority	Select the default tag priority for this port when adding a Tag to the untagged frames.
Queuing Mode	Select which Queuing mode for this port.
Queue Weighted	Setting Queue weighted (Low, Normal, Medium, High) if the "Queuing Mode" is "Weighted".

3.1.8.3 QoS Control List

This page lists the QCEs for a given QCL.

Frames can be classified by 4 different QoS classes: Low, Normal, Medium, and High.

The classification is controlled by a QoS assigned to each port.
A QCL consists of an ordered list of up to 12 QCEs.
Each QCE can be used to classify certain frames to a specific QoS class.
This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 DSCP or Tag Priority. Frames not matching any of the QCEs are classified to the default QoS Class for the port.



Label	Description
QCL#	Select a QCL to display a table that lists all the QCEs for that particular QCL.
QCE Type	Specifies which frame field the QCE processes to determine the QoS class of the frame. The following QCE types are supported: Ethernet Type: The Ethernet Type field. If frame is tagged, this is the Ethernet Type that follows the tag header. VLAN ID: VLAN ID. Only applicable if the frame is VLAN tagged. TCP/UDP Port: IPv4 TCP/UDP source/destination port. DSCP: IPv4 and IPv6 DSCP. ToS: The 3 precedence bit in the ToS byte of the IPv4/IPv6 header (also known as DS field). Tag Priority: User Priority. Only applicable if the frame is VLAN tagged or priority tagged.
Type Value	Indicates the value according to its QCE type.

	Ethernet Type: The field shows the Ethernet Type value. VLAN ID: The field shows the VLAN ID. TCP/UDP Port: The field shows the TCP/UDP port range. DSCP: The field shows the IPv4/IPv6 DSCP value.
Traffic Class	The QoS class associated with the QCE.
Modification Buttons	You can modify each QCE in the table using the following buttons: : Inserts a new QCE before the current row. : Edits the QCE. : Moves the QCE up the list. : Moves the QCE down the list. : Deletes the QCE. : The lowest plus sign adds a new entry at the bottom of the list of QCL.

3.1.8.4 QoS Statistics

This page provides statistics for the different queues for all switch ports.

Queuing Counters

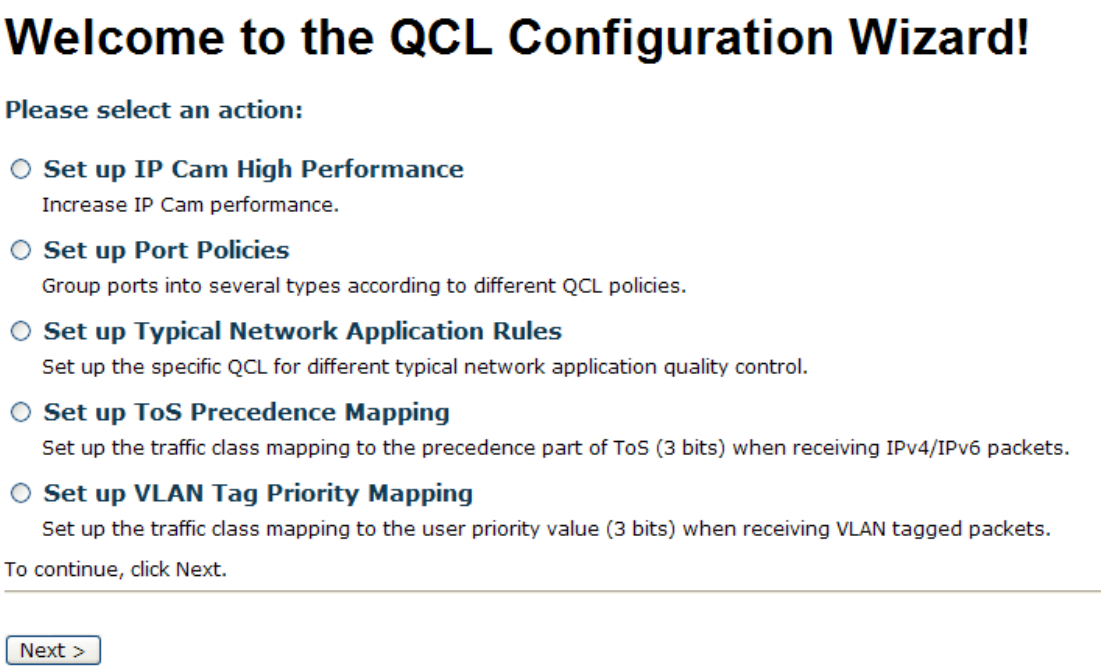
Auto-refresh ☐ Refresh Clear

Port	Low Queue		Normal Queue		Medium Queue		High Queue	
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	1423	0	0	0	0	0	0	990
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0

Label	Description
Port	The logical port for the settings contained in the same row.
Low Queue	There are 4 QoS queues per port with strict or weighted queuing scheduling. This is the lowest priority queue.
Normal Queue	This is the normal priority queue of the 4 QoS queues. It has higher priority than the "Low Queue".
Medium Queue	This is the medium priority queue of the 4 QoS queues. It has higher priority than the "Normal Queue".
High Queue	This is the highest priority queue of the 4 QoS queues.
Receive / Transmit	The number of received and transmitted packets per port.

3.1.8.5 Wizard

This handy wizard helps you set up a QCL quickly.


Welcome to the QCL Configuration Wizard!
Please select an action:
Set up IP Cam High Performance
Increase IP Cam performance.
Set up Port Policies
Group ports into several types according to different QCL policies.
Set up Typical Network Application Rules
Set up the specific QCL for different typical network application quality control.
Set up ToS Precedence Mapping
Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets.
Set up VLAN Tag Priority Mapping
Set up the traffic class mapping to the user priority value (3 bits) when receiving VLAN tagged packets.
To continue, click Next.
Next >

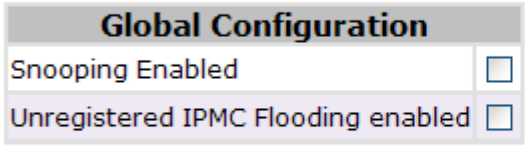
Label	Description
Set up Port Policies	Group ports into several types according to different QCL policies.
Set up Typical Network Application Rules	Set up the specific QCL for different typical network application quality control.
Set up ToS Precedence Mapping	Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets.
Set up VLAN Tag Priority Mapping	Set up the traffic class mapping to the User Priority value (3 bits) when receiving VLAN tagged packets.

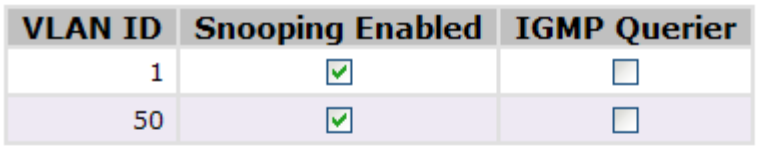
3.1.9 IGMP Snooping

3.1.9.1 IGMP Snooping

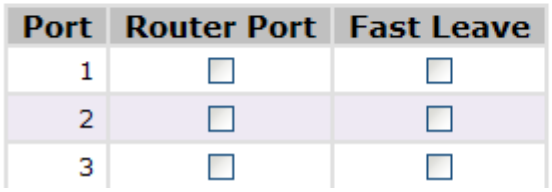
This page provides IGMP Snooping related configuration.

IGMP Snooping Configuration



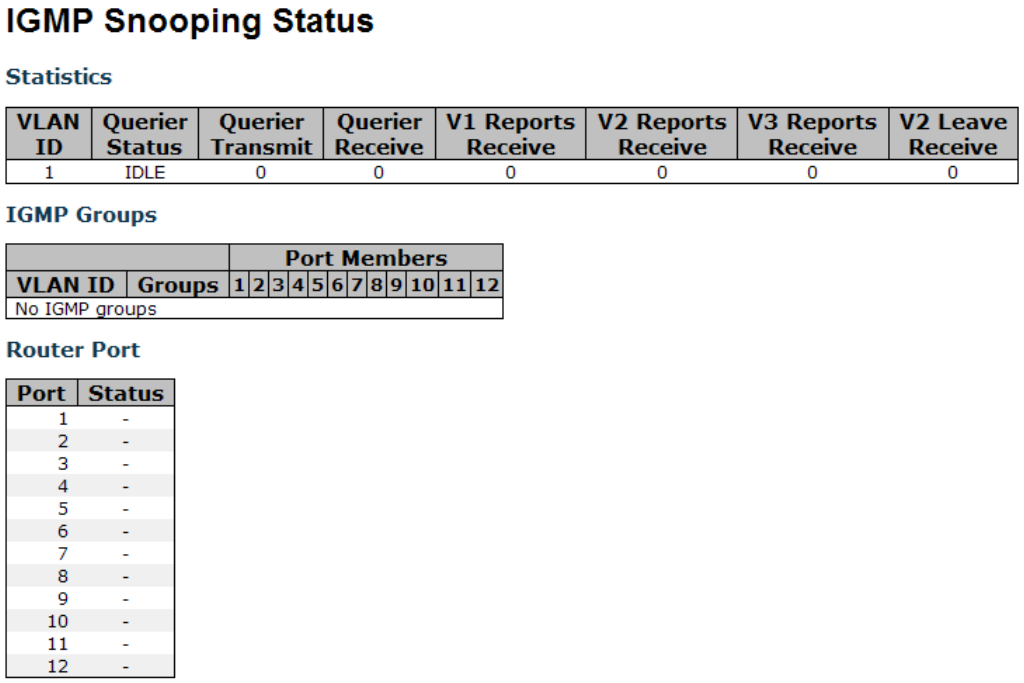


Port Related Configuration



Label	Description
Snooping Enabled	Enable the Global IGMP Snooping.
Unregistered IPMC Flooding enabled	Enable unregistered IPMC traffic flooding.
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enabled	Enable the per-VLAN IGMP Snooping.
IGMP Querier	Enable the IGMP Querier in the VLAN. The Querier will send out if no Querier received in 255 seconds after IGMP Querier Enabled. Each Querier's interval is 125 second, and it will stop act as an IGMP Querier if received any Querier from other devices.
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Enable the fast leave on the port.

3.1.9.2 IGMP Snooping Status



IGMP Snooping Status

Statistics

VLAN ID	Querier Status	Querier Transmit	Querier Receive	V1 Reports Receive	V2 Reports Receive	V3 Reports Receive	V2 Leave Receive
1	IDLE	0	0	0	0	0	0

IGMP Groups

		Port Members										
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12
No IGMP groups													

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-

Label	Description
VLAN ID	The VLAN ID of the entry.
Groups	The present IGMP groups. Max. Are 128 groups for each VLAN.
Port Members	The ports that are members of the entry.
Querier Status	Show the Querier status is "ACTIVE" or "IDLE".
Querier Receive	The number of Transmitted Querier.
V1 Reports Receive	The number of Received V1 Reports.
V2 Reports Receive	The number of Received V2 Reports.
V3 Reports Receive	The number of Received V3 Reports.
V2 Leave Receive	The number of Received V2 Leave.
Refresh	Click to refresh the page immediately.
Clear	Clears all Statistics counters.
Auto-refresh ☐	Check this box to enable an automatic refresh of the page at regular intervals.

3.1.10 Security

3.1.10.1 ACL

3.1.10.1.1 Ports

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

ACL Ports Configuration

Refresh Clear

Port	Policy ID	Action	Rate Limiter ID	Port Copy	Logging	Shutdown	Counter
1	1	Permit	Disabled	Disabled	Disabled	Disabled	0
2	1	Permit	Disabled	Disabled	Disabled	Disabled	0
3	1	Permit	Disabled	Disabled	Disabled	Disabled	0
4	1	Permit	Disabled	Disabled	Disabled	Disabled	0
5	1	Permit	Disabled	Disabled	Disabled	Disabled	0
6	1	Permit	Disabled	Disabled	Disabled	Disabled	0
7	1	Permit	Disabled	Disabled	Disabled	Disabled	1801
8	1	Permit	Disabled	Disabled	Disabled	Disabled	0
9	1	Permit	Disabled	Disabled	Disabled	Disabled	0
10	1	Permit	Disabled	Disabled	Disabled	Disabled	0
11	1	Permit	Disabled	Disabled	Disabled	Disabled	0
12	1	Permit	Disabled	Disabled	Disabled	Disabled	0

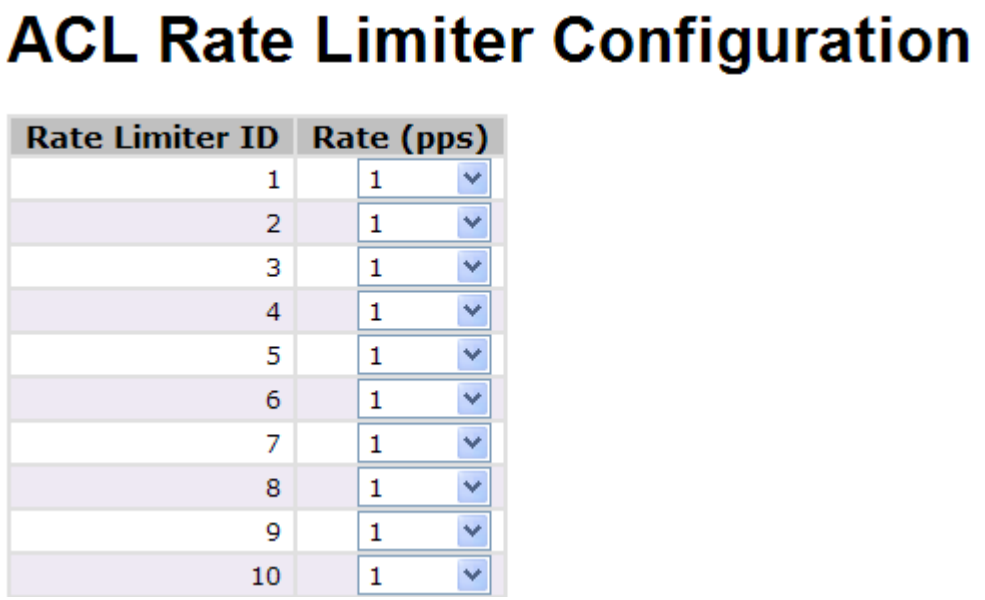
Save Reset

Label	Description
Port	The logical port for the settings contained in the same row.
Policy ID	Select the policy to apply to this port. The allowed values are 1 through 8. The default value is 1.
Action	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".
Rate Limiter ID	Select which rate limiter to apply to this port. The allowed values are Disabled or the values 1 through 15. The default value is "Disabled".
Port Copy	Select which port frames are copied to. The allowed values are Disabled or a specific port number. The default value is "Disabled".
Logging	Specify the logging operation of this port. The allowed values are: Enabled: Frames received on the port are stored in the System Log. Disabled: Frames received on the port are not logged. The default value is "Disabled". Please note that the System Log memory size and logging rate is limited.

Shutdown	Specify the port shut down operation of this port. The allowed values are: Enabled: If a frame is received on the port, the port will be disabled. Disabled: Port shut down is disabled. The default value is "Disabled".
Counter	Counts the number of frames that match this ACE.

3.1.10.1.2 Rate Limiters

Configure the rate limiter for the ACL of the switch.

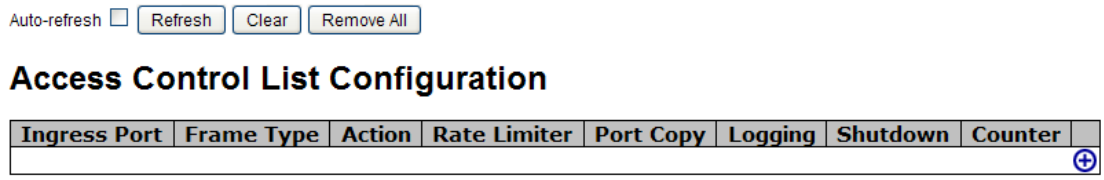


Label	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
Rate	The rate unit is packet per second (pps), configure the rate as 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K. The 1 kpps is actually 1002.1 pps.

3.1.10.1.3 Configuration

This page shows the Access Control List (ACL), which is made up of the ACEs defined for this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 128.

Click on the lowest plus sign to add a new ACE to the list.



Label	Description
Ingress Port	Indicates the ingress port of the ACE. Possible values are: Any: The ACE will match any ingress port. Policy: The ACE will match ingress ports with a specific policy. Port: The ACE will match a specific ingress port.
Frame Type	Indicates the frame type of the ACE. Possible values are: Any: The ACE will match any frame type.

	E Type: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. ARP: The ACE will match ARP/RARP frames. IPv4: The ACE will match all IPv4 frames. IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol. IPv4/UDP: The ACE will match IPv4 frames with UDP protocol. IPv4/TCP: The ACE will match IPv4 frames with TCP protocol. IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.
Action	Indicates the forwarding action of the ACE. Permit: Frames matching the ACE may be forwarded and learned. Deny: Frames matching the ACE are dropped.
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 15. When Disabled is displayed, the rate limiter operation is disabled.
Port Copy	Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port copy operation is disabled.
Logging	Indicates the logging operation of the ACE. Possible values are: Enabled: Frames matching the ACE are stored in the System Log. Disabled: Frames matching the ACE are not logged. Please note that the System Log memory size and logging rate is limited.
Shutdown	Indicates the port shut down operation of the ACE. Possible values are: Enabled: If a frame matches the ACE, the ingress port will be disabled. Disabled: Port shut down is disabled for the ACE.
Counter	The counter indicates the number of times the ACE was hit by a frame.
Modification Buttons	You can modify each ACE (Access Control Entry) in the table using the following buttons: ⊕ : Inserts a new ACE before the current row. ⓔ : Edits the ACE row. ⊛ : Moves the ACE up the list.

	: Moves the ACE down the list. : Deletes the ACE. : The lowest plus sign adds a new entry at the bottom of the ACE listings.

Configure an ACE (Access Control Entry) on this page.

An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type that you selected.
A frame that hits this ACE matches the configuration that is defined here.

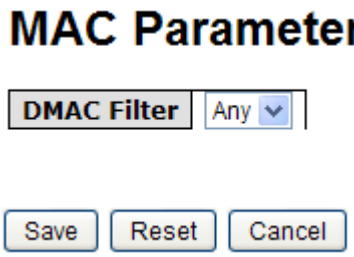
ACE Configuration

Ingress Port	Any
Frame Type	Any

Action	Permit
Rate Limiter	Disabled
Port Copy	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

Label	Description
Ingress Port	Select the ingress port for which this ACE applies. Any: The ACE applies to any port. Port n: The ACE applies to this port number, where n is the number of the switch port. Policy n: The ACE applies to this policy number, where n can range from 1 through 8.
Frame Type	Select the frame type for this ACE. These frame types are mutually exclusive. Any: Any frame can match this ACE. Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 descripts the value of Length/Type Field specifications should be greater than or equal to 1536 decimal (equal to 0600 hexadecimal). ARP: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with Ethernet type. IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames

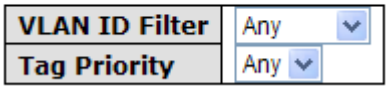
	won't match the ACE with Ethernet type.
Action	Specify the action to take with a frame that hits this ACE. Permit: The frame that hits this ACE is granted permission for the ACE operation. Deny: The frame that hits this ACE is dropped.
Rate Limiter	Specify the rate limiter in number of base units. The allowed range is 1 to 15. Disabled indicates that the rate limiter operation is disabled.
Port Copy	Frames that hit the ACE are copied to the port number specified here. The allowed range is the same as the switch port number range. Disabled indicates that the port copy operation is disabled.
Logging	Specify the logging operation of the ACE. The allowed values are: Enabled: Frames matching the ACE are stored in the System Log. Disabled: Frames matching the ACE are not logged. Please note that the System Log memory size and logging rate is limited.
Shutdown	Specify the port shut down operation of the ACE. The allowed values are: Enabled: If a frame matches the ACE, the ingress port will be disabled. Disabled: Port shut down is disabled for the ACE.
Counter	The counter indicates the number of times the ACE was hit by a frame.



Label	Description
SMAC Filter	(Only displayed when the frame type is Ethernet Type or ARP.) Specify the source MAC filter for this ACE. Any: No SMAC filter is specified. (SMAC filter status is "don't-care".) Specific: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.

SMAC Value	When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this SMAC value.
DMAC Filter	Specify the destination MAC filter for this ACE. Any: No DMAC filter is specified. (DMAC filter status is "don't-care".) MC: Frame must be multicast. BC: Frame must be broadcast. UC: Frame must be unicast. Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.
DMAC Value	When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this DMAC value.

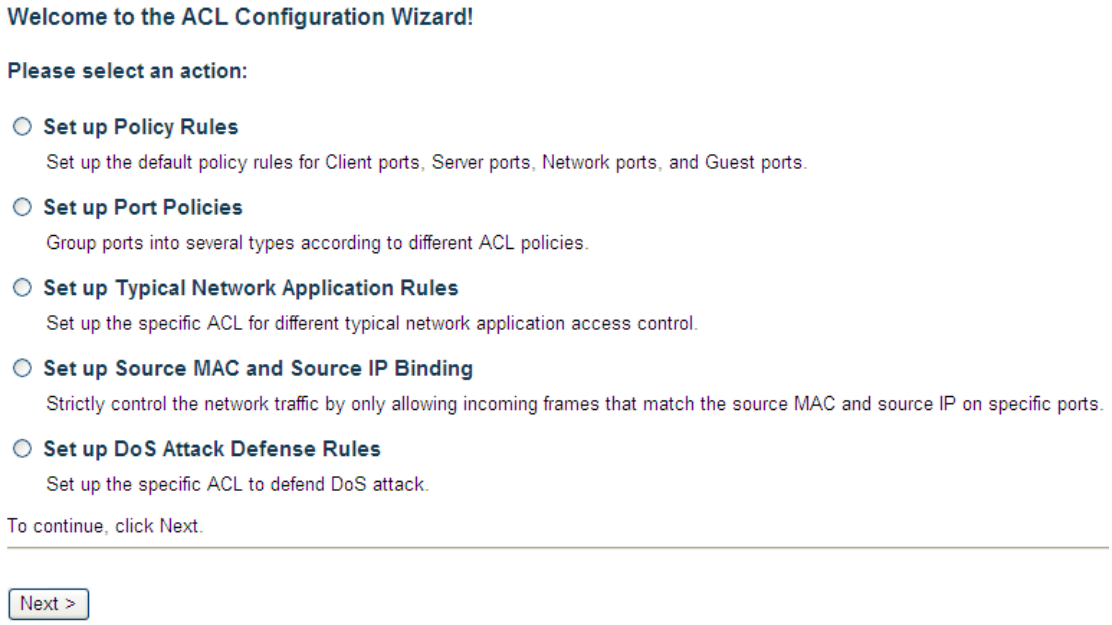
VLAN Parameters



Label	Description
VLAN ID Filter	Specify the VLAN ID filter for this ACE. Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".) Specific: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.
VLAN ID	When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.
Tag Priority	Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7. The value Any means that no tag priority is specified (tag priority is "don't-care".)

3.1.10.1.4 Wizard

This handy wizard helps you set up an ACL quickly.


Welcome to the ACL Configuration Wizard!
Please select an action:
Set up Policy Rules
Set up the default policy rules for Client ports, Server ports, Network ports, and Guest ports.
Set up Port Policies
Group ports into several types according to different ACL policies.
Set up Typical Network Application Rules
Set up the specific ACL for different typical network application access control.
Set up Source MAC and Source IP Binding
Strictly control the network traffic by only allowing incoming frames that match the source MAC and source IP on specific ports.
Set up DoS Attack Defense Rules
Set up the specific ACL to defend DoS attack.
To continue, click Next.
Next >

Label	Description
Set up Policy Rules	Set up the default policy rules for Client ports, Server ports, Network ports and Guest ports.
Set up Port Policies	Group ports into several types according to different ACL policies.
Set up Typical Network Application Rules	Set up the specific ACL for different typical network application access control.
Set up Source MAC and Source IP Binding	Strictly control the network traffic by only allowing incoming frames that match the source IP and source MAC on specific port.
Set up DoS Attack Defense Rules	Strictly control the network traffic by only allowing incoming frames that match the source IP and source MAC on specific port.

3.1.10.2 802.1x

This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the Authentication configuration page.

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1 X authentications.

Overview of 802.1X (Port-Based) Authentication

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switches are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS servers are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Note: Suppose two backend servers are enabled and that the server timeout is configured to

X seconds (using the Authentication configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

Overview of MAC-Based Authentication

Unlike 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using static entries into the MAC Table. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users, equipment whose MAC address is a valid RADIUS user can be used by anyone, and only the MD5-Challenge method is supported.

3.1.10.2.1 Configuration

The 802.1X and MAC-Based Authentication configuration consists of two sections, a system- and a port-wide

Port Security Configuration

System Configuration

Mode	Disabled
Reauthentication Enabled	☐
Reauthentication Period	3600 seconds
EAP Timeout	30 seconds
Age Period	300 seconds
Hold Time	10 seconds

Port Configuration

Port	Admin State	Port State	Max Clients		Restart	
1	Authorized	Disabled	All	112	Reauthenticate	Reinitialize
2	Authorized	Disabled	All	112	Reauthenticate	Reinitialize
3	Authorized	Disabled	All	112	Reauthenticate	Reinitialize
4	Authorized	Disabled	All	112	Reauthenticate	Reinitialize
5	Authorized	Disabled	All	112	Reauthenticate	Reinitialize

Label	Description
Mode	Indicates if 802.1X and MAC-based authentication is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.
Re-authentication Enabled	If checked, clients are re-authenticated after the interval specified by the Re-authentication Period. Re-authentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port. For MAC-based ports, re-authentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Age Period below).
Re-authentication Period	Determines the period, in seconds, after which a connected client must be re-authenticated. This is only active if the Re-authentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.
EAP Timeout	Determines the time the switch shall wait for the supplicant response before retransmitting a packet. Valid values are in the range 1 to 255 seconds. This has no effect for MAC-based ports.

Age Period	This setting applies to ports running MAC-based authentication, only. Suppose a client is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch that runs MAC-based authentication, and suppose the client gets successfully authenticated. Now assume that the client powers down his PC. What should make the switch forget about the authenticated client? Re-authentication will not solve this problem, since this doesn't require the client to be present, as discussed under Re-authentication Enabled above. The solution is aging of authenticated clients. The Age Period, which can be set to a number between 10 and 1000000 seconds, works like this: A timer is started when the client gets authenticated. After half the age period, the switch starts looking for frames sent by the client. If another half age period elapses and no frames are seen, the client is considered removed from the system, and it will have to authenticate again the next time a frame is seen from it. If, on the other hand, the client transmits a frame before the second half of the age period expires, the switch will consider the client alive, and leave it authenticated. Therefore, an age period of T will require the client to send frames more frequent than T/2 for him to stay authenticated.
Hold Time	This setting applies to ports running MAC-based authentication, only. If the RADIUS server denies a client access, or a RADIUS server request times out (according to the timeout specified on the Authentication configuration page), the client is put on hold in the Unauthorized state. In this state, frames from the client will not cause the switch to attempt to re-authenticate the client. The Hold Time, which can be set to a number between 10 and 1000000 seconds, determines the time after an EAP Failure indication or RADIUS timeout that a client is not allowed access.
Port	The port number for which the configuration below applies.
Admin State	Sets the authentication mode to one of the following options (only used when 802.1X or MAC-based authentication is globally enabled): Auto: Requires an 802.1X-aware client (supplicant) to be

	authorized by the authentication server. Clients that are not 802.1X-aware will be denied access. Authorized: Forces the port to grant access to all clients, 802.1X-aware or not. The switch transmits an EAPOL Success frame when the port links up. Unauthorized: Forces the port to deny access to all clients, 802.1X-aware or not. The switch transmits an EAPOL Failure frame when the port links up. MAC-Based: Enables MAC-based authentication on the port. The switch doesn't transmit or accept EAPOL frames on the port. Flooded frames and broadcast traffic will be transmitted on the port, whether or not clients are authenticated on the port, whereas unicast traffic against an unsuccessfully authenticated client will be dropped. Clients that are not (yet) successfully authenticated will not be allowed to transmit frames of any kind.
Port State	The current state of the port. It can undertake one of the following values: Disabled: 802.1X and MAC-based authentication is globally disabled. Link Down: 802.1X or MAC-based authentication is enabled, but there is no link on the port. Authorized: The port is authorized. This is the case when 802.1 X authentications is enabled, the port has link, and the Admin State is "Auto" and the supplicant is authenticated or the Admin State is "Authorized". Unauthorized: The port is unauthorized. This is the case when 802.1X authentication is enabled, the port has link, and the Admin State is "Auto", but the supplicant is not (yet) authenticated or the Admin State is "Unauthorized". X Auth/Y Unauth: X clients are currently authorized and Y is unauthorized. This state is shown when 802.1X and MAC-based authentication is globally enabled and the Admin State is set to "MAC-Based".
Max Clients	This setting applies to ports running MAC-based authentication, only. The maximum number of clients allowed on a given port can be configured through the list-box and edit-control for this setting.

	Choosing the value "All" from the list-box allows the port to consume up to 48 client state-machines. Choosing the value "Specific" from the list-box opens up for entering a specific number of maximum clients on the port (1 to 48). The switch is "born" with a pool of state-machines, from which all ports draw whenever a new client is seen on the port. When a given port's maximum is reached (both authorized and unauthorized clients count), further new clients are disallowed access. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available state-machines.
Restart	Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is "Auto" or "MAC-Based". Clicking these buttons will not cause settings changed on the page to take effect. Re-authenticate: Schedules a re-authentication to whenever the quiet-period of the port runs out (port-based authentication). For MAC-based authentication, re-authentication will be attempted immediately. The button only has effect for successfully authenticated ports/clients and will not cause the port/client to get temporarily unauthorized. Reinitialize: Forces a re-initialization of the port/clients and thereby a re-authentication immediately. The port/clients will transfer to the unauthorized state while the re-authentication is ongoing.

3.1.10.2.2 Status

Label	Description
Port	The switch port number. Click to navigate to detailed 802.1X statistics for this port.
State	The current state of the port. Refer to IEEE 802.1X Port State for a description of the individual states.
Last Source	The source MAC address carried in the most recently received EAPOL frame for port-based authentication, and the most recently received frame from a new client for MAC-based authentication.
Last ID	The user name (supplicant identity) carried in the most recently received Resp/ID EAPOL frame for port-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

3.1.10.2.3 Statistics

This page provides detailed IEEE 802.1X statistics for a specific switch port running port-based authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only. Use the port select box to select which port details to be displayed.

802.1X Statistics Port 1

Port 1 Auto-refresh Refresh Clear

Receive EAPOL Counters		Transmit EAPOL Counters	
Total	0	Total	0
Response ID	0	Request ID	0
Responses	0	Requests	0
Start	0		
Logoff	0		
Invalid Type	0		
Invalid Length	0		
Receive Backend Server Counters		**Transmit Backend Server Counters**	
Access Challenges	0	Responses	0
Other Requests	0		
Auth. Successes	0		
Auth. Failures	0		
Last Supplicant Info			
Version			0
Source			
Identity			

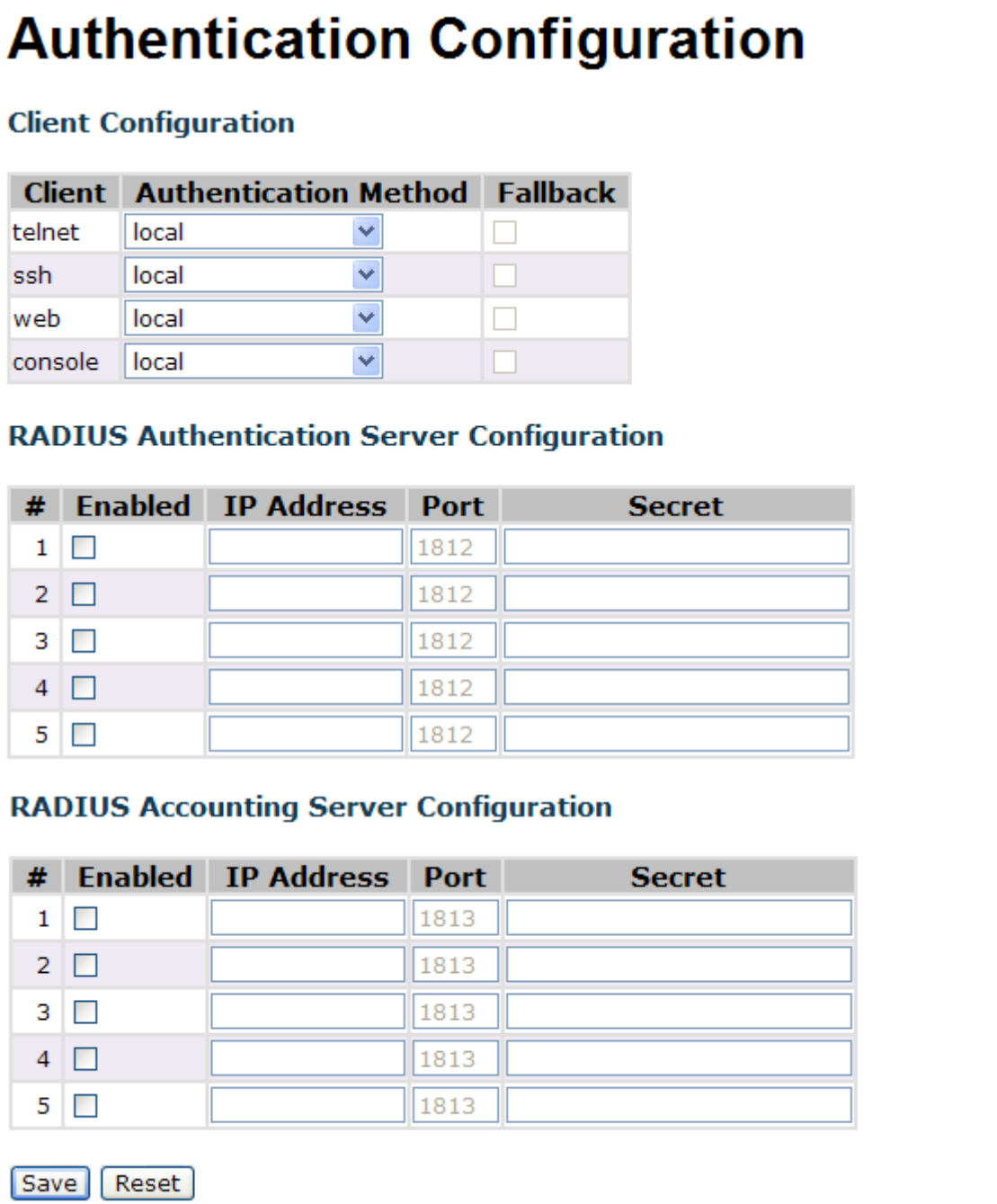
Label	Description
EAPOL Counters	These counters are not available for MAC-based ports. Supplicant frame counter statistics. There are seven receive frame counters and three transmit frame counters.
Backend Server Counters	Backend server frame counter statistics. For MAC-based ports there are two tables containing backend server counters. The left-most shows a summary of all backend server counters on this port. The right-most shows backend server counters for the currently selected client, or dashes if no client is selected or available. A client can be selected from the list of authorized/unauthorized clients below the two counter tables. There are slight differences in the interpretation of the counters between port- and MAC-based authentications as shown below.

EAPOL Counters

Direction	Name	IEEE Name	Description
Rx	Total	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
Rx	Response ID	dot1xAuthEapolRespIdFramesRx	The number of valid EAP Resp/ID frames that have been received by the switch.
Rx	Responses	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Resp/ID frames) that have been received by the switch.
Rx	Start	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
Rx	Logoff	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL logoff frames that have been received by the switch.
Rx	Invalid Type	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
Rx	Invalid Length	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
Tx	Total	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
Tx	Request ID	dot1xAuthEapolReqIdFramesTx	The number of EAP initial request frames that have been transmitted by the switch.
Tx	Requests	dot1xAuthEapolReqFramesTx	The number of valid EAP Request frames (other than initial request frames) that have been transmitted by the switch.

<table>
<tr><td></td><td>
<table>
<tr><th colspan="4">Backend Server Counters</th></tr>
<tr><th>Direction</th><th>Name</th><th>IEEE Name</th><th>Description</th></tr>
<tr><td>Rx</td><td>Access Challenges</td><td>dot1xAuthBackendAccessChallenges</td><td>Port-based:
Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch.
MAC-based:
Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).</td></tr>
<tr><td>Rx</td><td>Other Requests</td><td>dot1xAuthBackendOtherRequestsToSupplicant</td><td>Port-based:
Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method.
MAC-based:
Not applicable.</td></tr>
<tr><td>Rx</td><td>Auth. Successes</td><td>dot1xAuthBackendAuthSuccesses</td><td>Port- and MAC-based:
Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.</td></tr>
<tr><td>Rx</td><td>Auth. Failures</td><td>dot1xAuthBackendAuthFails</td><td>Port- and MAC-based:
Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.</td></tr>
<tr><td>Tx</td><td>Responses</td><td>dot1xAuthBackendResponses</td><td>Port-based:
Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted.
MAC-based:
Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.</td></tr>
</table>
</td></tr>
<tr><td>Last Supplicant/Client Info</td><td>For MAC-based ports, this section is embedded in the backend server counter's section.
Information about the last supplicant/client that attempted to authenticate.
<table>
<tr><th colspan="3">Last Supplicant/Client Info</th></tr>
<tr><th>Name</th><th>IEEE Name</th><th>Description</th></tr>
<tr><td>Version</td><td>dot1xAuthLastEapolFrameVersion</td><td>Port-based:
The protocol version number carried in the most recently received EAPOL frame.
MAC-based:
Not applicable.</td></tr>
<tr><td>Source</td><td>dot1xAuthLastEapolFrameSource</td><td>Port-based:
The source MAC address carried in the most recently received EAPOL frame.
MAC-based:
Not applicable.</td></tr>
<tr><td>Identity or (Last) Client</td><td>-</td><td>Port-based:
The user name (supplicant identity) carried in the most recently received Resp/ID EAPOL frame.
MAC-based:
The MAC address of the last client that attempted to authenticate (left-most table), or the MAC address of the currently selected client (right-most table).</td></tr>
</table>
</td></tr>
<tr><td>Clients attached to this port</td><td>This table is only available for MAC-based ports
Each row in the table represents a MAC-based client on the port, and there are three parameters for each client:
MAC Address:
Shows the MAC address of the client, which is also used as the password in the authentication process against the backend server. Clicking the link causes the client's backend server counters to be shown in the right-most backend server counters table above. If no clients are attached, it shows No clients attached.
State:
Shows whether the client is authorized or unauthorized. As long as the backend server hasn't successfully authenticated a client, it is unauthorized.
Last Authentication:
Show the date and time of the last authentication of the client. This gets updated for every re-authentication of the client.</td></tr>
</table>

3.1.10.2.4 Authentication



Client Configuration

The table has one row for each Client and a number of columns, which are:

Label	Description
Client	The Client for which the configuration below applies.
Authentication	Authentication Method can be set to one of the following values:

Method	None: authentication is disabled and login is not possible. Local: use the local user database on the switch stack for authentication. Radius: use a remote RADIUS server for authentication. Tacacs+: use a remote TACACS+ server for authentication.
Fallback	Enable fallback to local authentication by checking this box. If none of the configured authentication servers are alive, the local user database is used for authentication. This is only possible if the Authentication Method is set to something else than 'none or 'local'.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Common Server Configuration

These setting are common for all of the Authentication Servers.

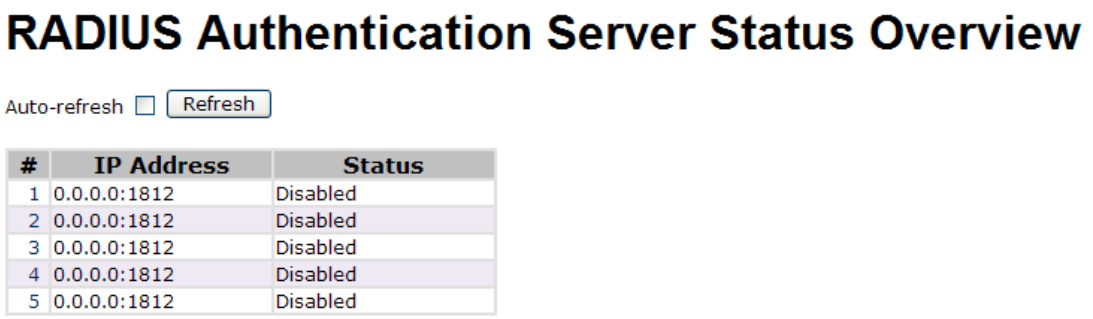
Label	Description
Timeout	The Timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server. If the server does not reply within this timeframe, we will consider it to be dead and continue with the next enabled server (if any). RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.
Dead Time	The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

3.1.10.2.5 RADIUS Status

RADIUS Authentication Server Configuration

The table has one row for each RADIUS Authentication Server and a number of columns, which are:

Label	Description
#	The RADIUS Authentication Server number for which the configuration below applies.
Enable	Enable the RADIUS Authentication Server by checking this box.
IP Address	Enable fallback to local authentication by checking this box. If none of the configured authentication servers are alive, the local user database is used for authentication. This is only possible if the Authentication Method is set to something else than 'none or 'local'.



Label	Description
#	The RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
State	The current state of the server. This field takes one of the following values: Disabled: The server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

	Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0:1813	Disabled
2	0.0.0.0:1813	Disabled
3	0.0.0.0:1813	Disabled
4	0.0.0.0:1813	Disabled
5	0.0.0.0:1813	Disabled

Label	Description
#	The RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
State	The current state of the server. This field takes one of the following values: Disabled: The server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

3.1.10.2.6 RADIUS Statistics

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client

MIB.

Use the server select box to switch between the backend servers to show details for.

RADIUS Authentication Statistics for Server #1 (0.0.0.0:1812)

Server #1 Auto-refresh Refresh Clear

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
State	Disabled		
Round-Trip Time	0 ms		

<table>
<tr><th>Label</th><th>Description</th></tr>
<tr><td>Packet Counters</td><td>RADIUS authentication server packet counter. There are seven receive and four transmit counters.
<table>
<tr><th>Direction</th><th>Name</th><th>RFC4668 Name</th><th>Description</th></tr>
<tr><td>Rx</td><td>Access Accepts</td><td>radiusAuthClientExtAccessAccepts</td><td>The number of RADIUS Access-Accept packets (valid or invalid) received from the server.</td></tr>
<tr><td>Rx</td><td>Access Rejects</td><td>radiusAuthClientExtAccessRejects</td><td>The number of RADIUS Access-Reject packets (valid or invalid) received from the server.</td></tr>
<tr><td>Rx</td><td>Access Challenges</td><td>radiusAuthClientExtAccessChallenges</td><td>The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.</td></tr>
<tr><td>Rx</td><td>Malformed Access Responses</td><td>radiusAuthClientExtMalformedAccessResponses</td><td>The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.</td></tr>
<tr><td>Rx</td><td>Bad Authenticators</td><td>radiusAuthClientExtBadAuthenticators</td><td>The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.</td></tr>
<tr><td>Rx</td><td>Unknown Types</td><td>radiusAuthClientExtUnknownTypes</td><td>The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.</td></tr>
<tr><td>Rx</td><td>Packets Dropped</td><td>radiusAuthClientExtPacketsDropped</td><td>The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.</td></tr>
<tr><td>Tx</td><td>Access Requests</td><td>radiusAuthClientExtAccessRequests</td><td>The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.</td></tr>
<tr><td>Tx</td><td>Access Retransmissions</td><td>radiusAuthClientExtAccessRetransmissions</td><td>The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.</td></tr>
<tr><td>Tx</td><td>Pending Requests</td><td>radiusAuthClientExtPendingRequests</td><td>The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.</td></tr>
<tr><td>Tx</td><td>Timeouts</td><td>radiusAuthClientExtTimeouts</td><td>The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.</td></tr>
</table></td></tr>
<tr><td>Other Info</td><td>This section contains information about the state of the server and the latest round-trip time.
<table>
<tr><th>Name</th><th>RFC4668 Name</th><th>Description</th></tr>
<tr><td>State</td><td>-</td><td>Shows the state of the server. It takes one of the following values:
<code>Disabled</code> : The selected server is disabled.
<code>Not Ready</code> : The server is enabled, but IP communication is not yet up and running.
<code>Ready</code> : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
<code>Dead (X seconds left)</code> : Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.</td></tr>
<tr><td>Round-Trip Time</td><td>radiusAuthClientExtRoundTripTime</td><td>The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.</td></tr>
</table></td></tr>
</table>

RADIUS Accounting Statistics for Server #1 (0.0.0.0:1813)

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
State	Disabled		
Round-Trip Time	0 ms		

Label	Description
Packet Counters	RADIUS accounting server packet counter. There are five receive and four transmit counters.
Other Info	This section contains information about the state of the server and the latest

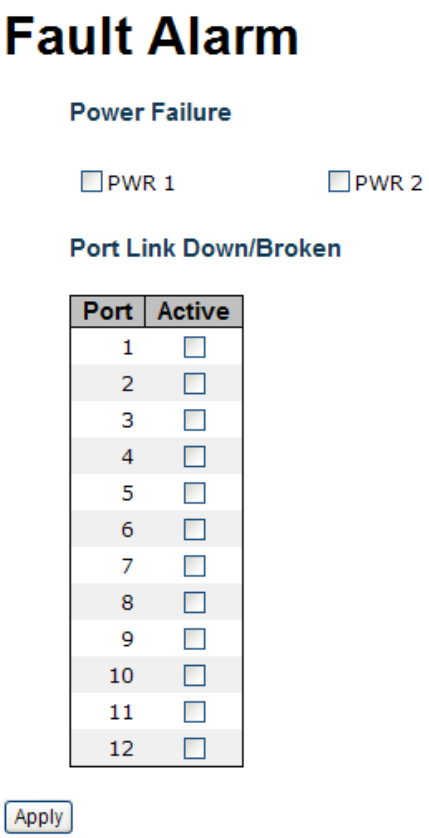
Direction	Name	RFC4670 Name	Description
Rx	Responses	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	Malformed Responses	radiusAccClientExtMalformedResponses	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or or unknown types are not included as malformed access responses.
Rx	Bad Authenticators	radiusAcctClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	Unknown Types	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	Packets Dropped	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx	Requests	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx	Retransmissions	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx	Pending Requests	radiusAccClientExtPendingRequests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.
Tx	Timeouts	radiusAccClientExtTimeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

Name	RFC4670 Name	Description
State	-	Shows the state of the server. It takes one of the following values: `Disabled` : The selected server is disabled. `Not Ready` : The server is enabled, but IP communication is not yet up and running. `Ready` : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. `Dead (X seconds left)` : Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAccClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

3.1.11 Warning

3.1.11.1 Fault Alarm

When any selected fault event is happened, the Fault LED in switch panel will light up and the electric relay will signal at the same time.



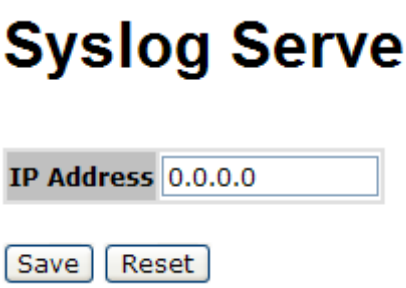
Fault Alarm interface

The following table describes the labels in this screen.

Label	Description
Power Failure	Mark the blank of PWR 1 or PWR 2 to monitor.
Port Link Down/Broken	Mark the blank of port 1 to port 12 to monitor.
Apply	Click "**Apply**" to set the configurations.

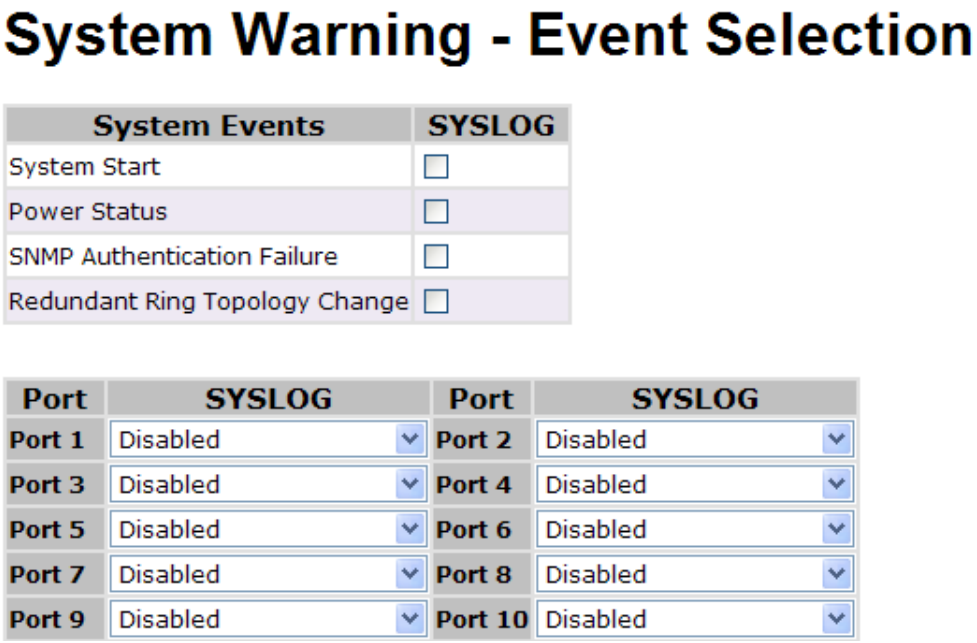
3.1.11.2 System warning

3.1.11.2.1 Syslog Setting



Label	Description
IP Address	User can input syslog server IP
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

3.1.11.3 Event Selection



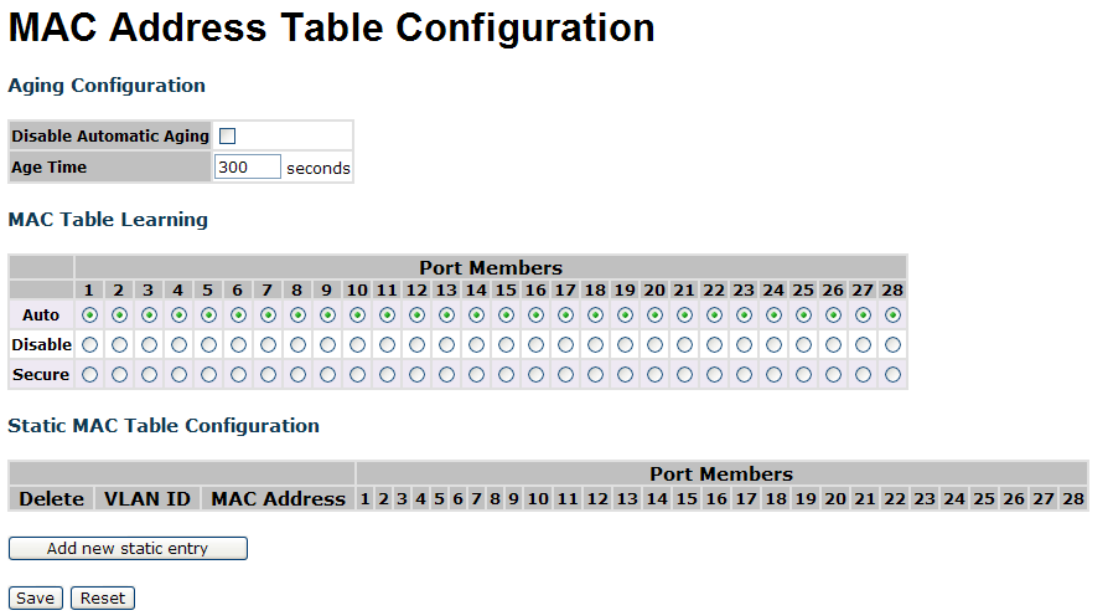
Label	Description
System Event	
System Start	Alert when system restart
Power Status	Alert when a power up or down
SNMP Authentication Failure	Alert when SNMP authentication failure.
Redundant Ring	Alert when Redundant Ring. topology changes.

Topology Change	
Port Event **SYSLOG event**	■ **Disable** ■ **Link Up** ■ **Link Down** ■ **Link Up & Link Down**
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

3.1.12 Monitor and Diagnostics

3.1.12.1 MAC Table - Configuration

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.


MAC Address Table Configuration
Aging Configuration
Disable Automatic Aging
Age Time
300
seconds
MAC Table Learning
Port Members
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
Auto
Disable
Secure
Static MAC Table Configuration
Delete
VLAN ID
MAC Address
Port Members
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
Add new static entry
Save
Reset

Aging Configuration

By default, dynamic entries are removed from the MAC after 300 seconds. This removal is also called aging.

Configure aging time by entering a value here in seconds; for example, **Age time** seconds.

The allowed range is 10 to 1000000 seconds.

Disable the automatic aging of dynamic entries by checking ☐ **Disable automatic aging**.

MAC Table Learning

If the learning mode for a given port is grayed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.

Each port can do learning based upon the following settings:

MAC Table Learning

	Port Members																											
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Auto	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉
Disable	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Label	Description
Auto	Learning is done automatically as soon as a frame with unknown SMAC is received.
Disable	No learning is done.
Secure	Only static MAC entries are learned, all other frames are dropped. Note: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

The maximum of 64 entries is for the whole stack, and not per switch.

The MAC table is sorted first by VLAN ID and then by MAC address.

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
MAC Address	The MAC address for the entry.
Port Members	Checkmarks indicate which ports are members of the entry.

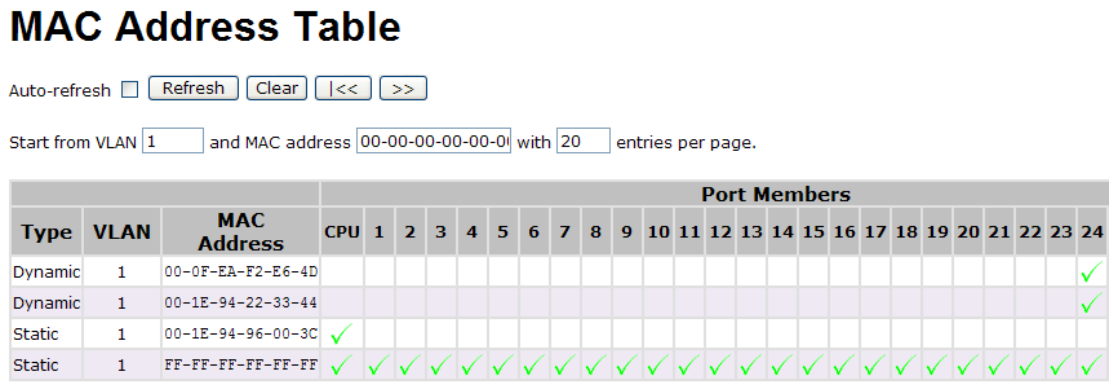
	Check or uncheck as needed to modify the entry.
Adding a New Static Entry	Click Add new static entry to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

3.1.12.2 MAC Table - MAC Table-

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The "Start from MAC address" and "VLAN" input fields allow the user to select the starting point in the MAC Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MAC Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "no more entries" is shown in the displayed table. Use the |<< button to start over.


MAC Address Table
Auto-refresh
Refresh
Clear
|<<
>>
Start from VLAN 1 and MAC address 00-00-00-00-00-0 with 20 entries per page.
Port Members
Type VLAN MAC Address CPU 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Dynamic 1 00-0F-EA-F2-E6-4D
Dynamic 1 00-1E-94-22-33-44
Static 1 00-1E-94-96-00-3C
Static 1 FF-FF-FF-FF-FF-FF

Label	Description
Type	Indicates whether the entry is a static or dynamic entry.
MAC address	The MAC address of the entry.
VLAN	The VLAN ID of the entry.

Port Members	The ports that are members of the entry.
Refresh	Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.
Clear	Flushes all dynamic entries.
|<<	Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.
>>	Updates the table, starting with the entry after the last entry currently displayed.

3.1.13 Port Statistics

3.1.13.1 Traffic Overview

This page provides an overview of general traffic statistics for all switch ports.

Port Statistics Overview

Auto-refresh ☐ Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0

Label	Description
Port	The logical port for the settings contained in the same row.

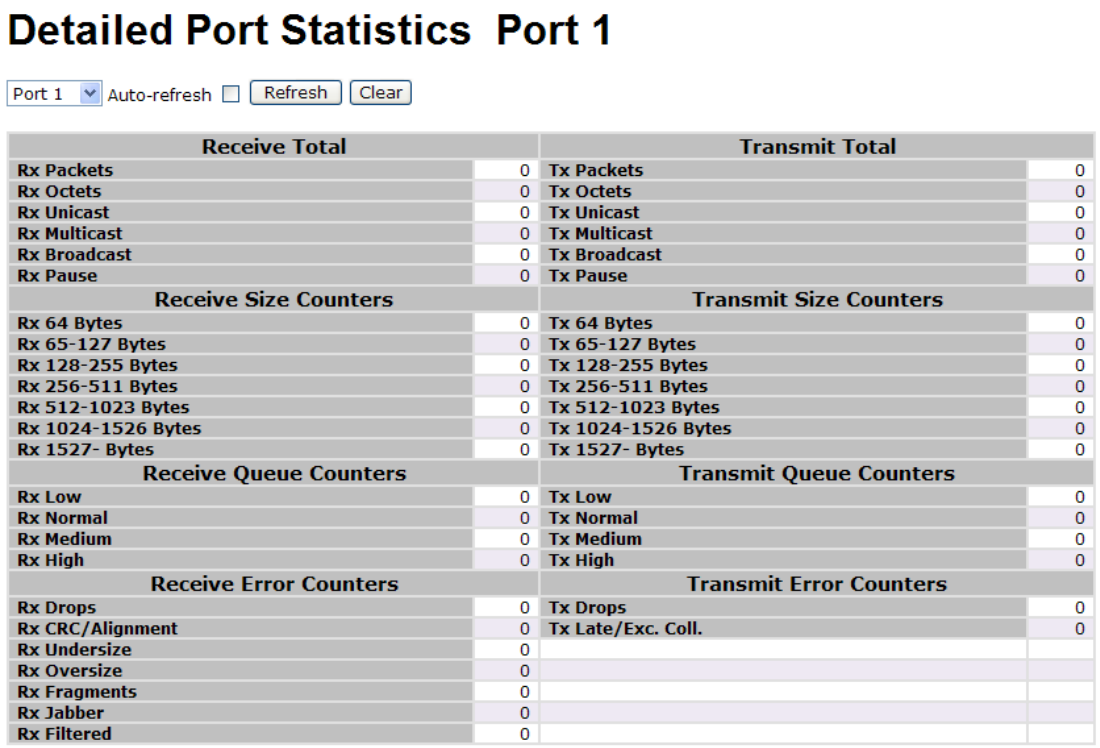
Packets	The number of received and transmitted packets per port.
Bytes	The number of received and transmitted bytes per port.
Errors	The number of frames received in error and the number of incomplete transmissions per port.
Drops	The number of frames discarded due to ingress or egress congestion.
Filtered	The number of received frames filtered by the forwarding process.
Auto-refresh ☐	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Updates the counters entries, starting from the current entry ID.
Clear	Flushes all counters entries.

3.1.13.2 Detailed statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

Detailed Statistics-Receive & Transmit Total



Label	Description
RX and TX Packets	The number of received and transmitted (good and bad) packets.
RX and TX Octets	The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
Rx and TX Unicast	The number of received and transmitted (good and bad) unicast packets.
RX and TX Multicast	The number of received and transmitted (good and bad) multicast packets.
RX and TX Broadcast	The number of received and transmitted (good and bad) broadcast packets.
RX and TX Pause	A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.
RX Drops	The numbers of frames dropped due to lack of receive buffers or egress congestion.
RX CRC/Alignment	The number of frames received with CRC or alignment errors.
RX Undersize	The number of short 1 frames received with valid CRC.
RX Oversize	The number of long 2 frames received with valid CRC.
RX Fragments	The number of short 1 frames received with invalid CRC.

RX Jabber	The number of long 2 frames received with invalid CRC.
RX Filtered	The number of received frames filtered by the forwarding process.
TX Drops	The number of frames dropped due to output buffer congestion.
TX Late / Exc.Coll.	The number of frames dropped due to excessive or late collisions.

3.1.14 Port Monitoring

Configure port Mirroring on this page.

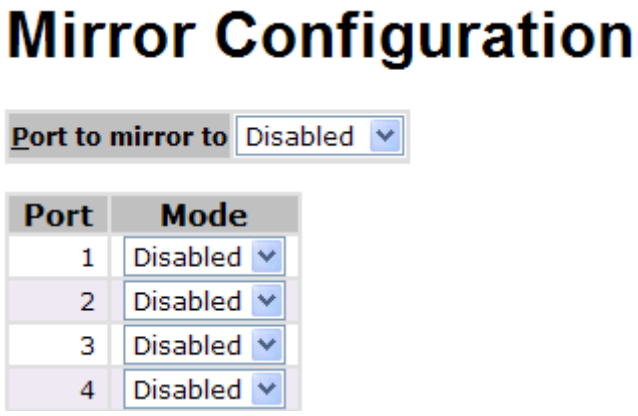
To debug network problems, selected traffic can be copied, or mirrored, to a mirror port where a frame analyzer can be attached to analyze the frame flow.

The traffic to be copied to the mirror port is selected as follows:

All frames received on a given port (also known as ingress or source mirroring).

All frames transmitted on a given port (also known as egress or destination mirroring).

Port to mirror; also known as the mirror port. Frames from ports that have either source (RX) or destination (TX) mirroring enabled are mirrored to this port. Disabled disables mirroring.



Label	Description
Port	The logical port for the settings contained in the same row.
Mode	Select mirror mode. RX only: Frames received at this port are mirrored to the mirror port. Frames transmitted are not mirrored. TX only: Frames transmitted from this port are mirrored to the mirror port. Frames received are not mirrored. Disabled: Neither frames transmitted nor frames received are mirrored. Enabled: Frames received and frames transmitted are mirrored to the mirror port.

	Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror TX frames for the mirror port. Because of this, mode for the selected mirror port is limited to Disabled or RX only.

3.1.15 System Log Information

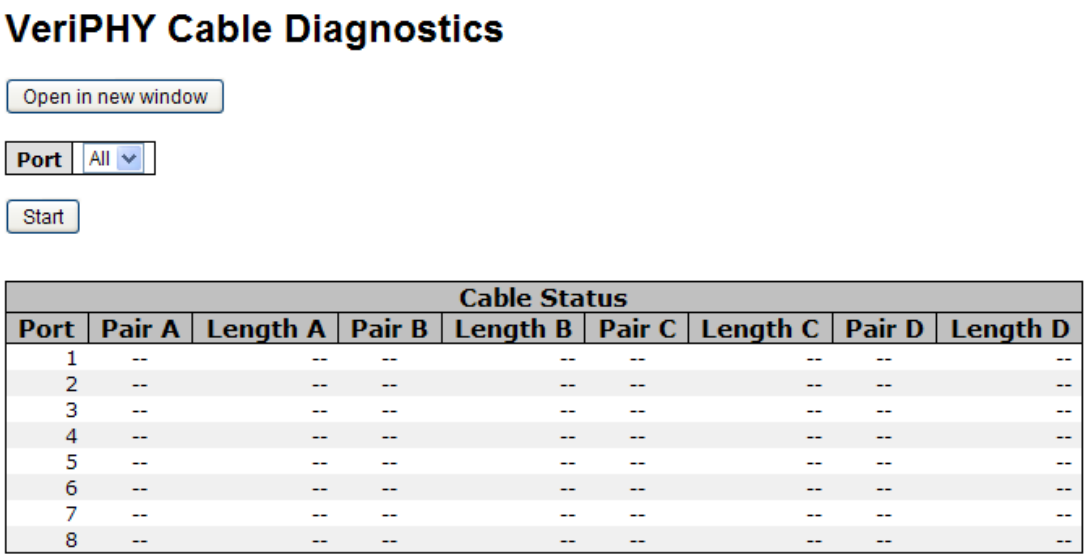
The switch system log information is provided here.

Label	Description
ID	The ID (>= 1) of the system log entry.
Level	The level of the system log entry. The following level types are supported: Info: Information level of the system log. Warning: Warning level of the system log. Error: Error level of the system log. All: All levels.
Time	The time of the system log entry.
Message	The MAC Address of this switch.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Updates the system log entries, starting from the current entry ID.
Clear	Flushes all system log entries.
|<<	Updates the system log entries, starting from the first available entry ID.
<<	Updates the system log entries, ending at the last entry currently displayed.

>>	Updates the system log entries, starting from the last entry currently displayed.
>>|	Updates the system log entries, ending at the last available entry ID.

3.1.16 Cable Diagnostics

This page is used for running the VeriPHY Cable Diagnostics.


VeriPHY Cable Diagnostics
Open in new window
Port
All
Start
Cable Status
Port Pair A Length A Pair B Length B Pair C Length C Pair D Length D
1 -- -- -- -- -- -- -- -- --
2 -- -- -- -- -- -- -- -- --
3 -- -- -- -- -- -- -- -- --
4 -- -- -- -- -- -- -- -- --
5 -- -- -- -- -- -- -- -- --
6 -- -- -- -- -- -- -- -- --
7 -- -- -- -- -- -- -- -- --
8 -- -- -- -- -- -- -- -- --

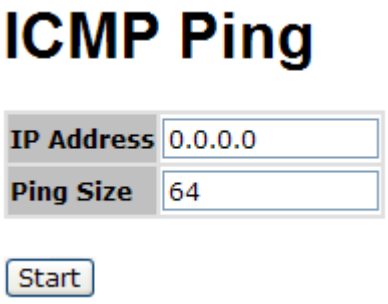
Press Start to run the diagnostics. This will take approximately 5 seconds. If all

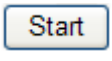
ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters.
10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

Label	Description
Port	The port where you are requesting VeriPHY Cable Diagnostics.
Cable Status	Port: Port number. Pair: The status of the cable pair. Length: The length (in meters) of the cable pair.

3.1.17 Ping

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.



After you press 

, 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING6 server: 10.10.132.20
64 bytes from: 10.10.132.20: icmp_seq=0, time=0ms

64 bytes from: 10.10.132.20: icmp_seq=1, time=0ms
64 bytes from: 10.10.132.20: icmp_seq=2, time=0ms
64 bytes from: 10.10.132.20: icmp_seq=3, time=0ms
64 bytes from: 10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad

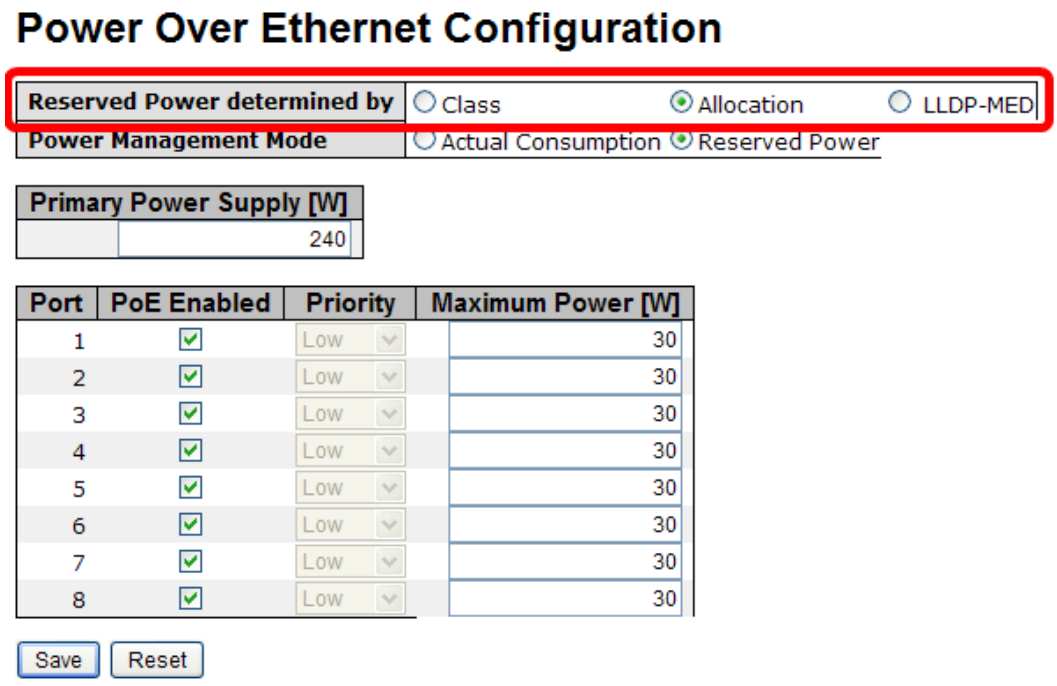
You can configure the following properties of the issued ICMP packets:

Label	Description
IP Address	The destination IP Address.
Ping Size	The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.

3.1.18 Power Over Ethernet (PoE)

3.1.18.1 PoE Configuration - Reserved Power determined

There are three modes for configuring how the ports/PDs may reserve power.



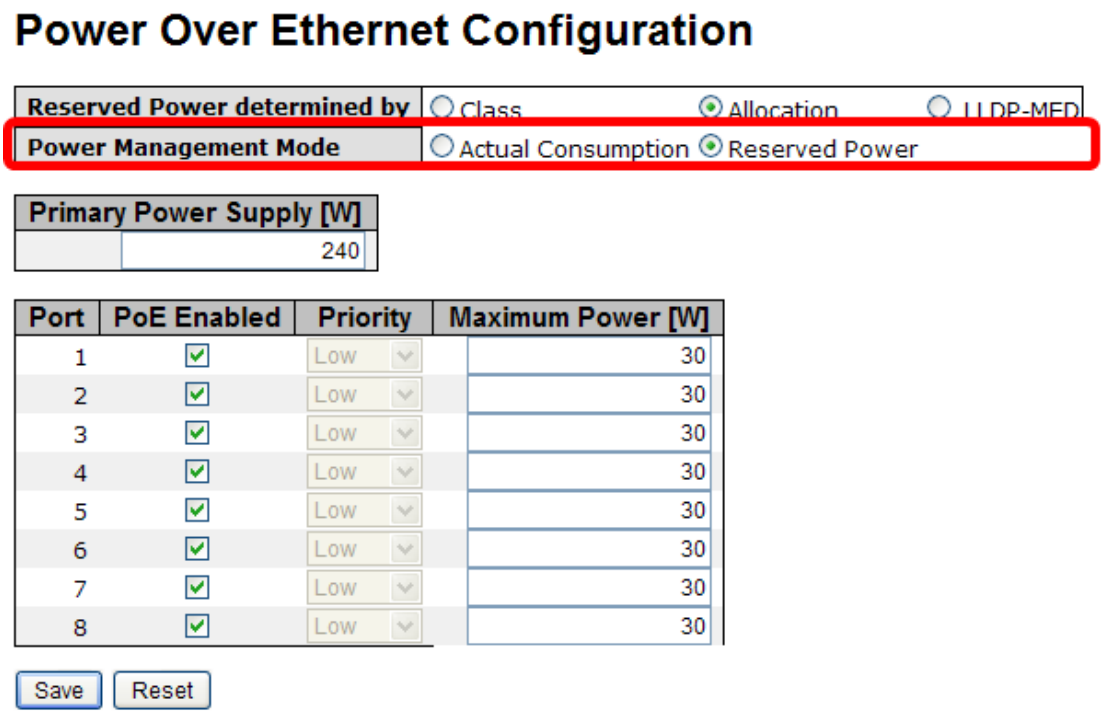
Label	Description
Allocated mode	In this mode the user allocates the amount of power that each

	port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields.
Class mode	In this mode each port automatic determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Three different port classes exist and one for 4, 7 and 15.4 Watts. (In this mode the Maximum Power fields have no effect.)
LLDP-MED mode	This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode.(In this mode the Maximum Power fields have no effect)

(For all modes: If a port uses more power than the reserved power for the port, the port is shut down.)

3.1.18.2 PoE Configuration - Power management Mode

There are 2 modes for configuring when to the ports is shut down.

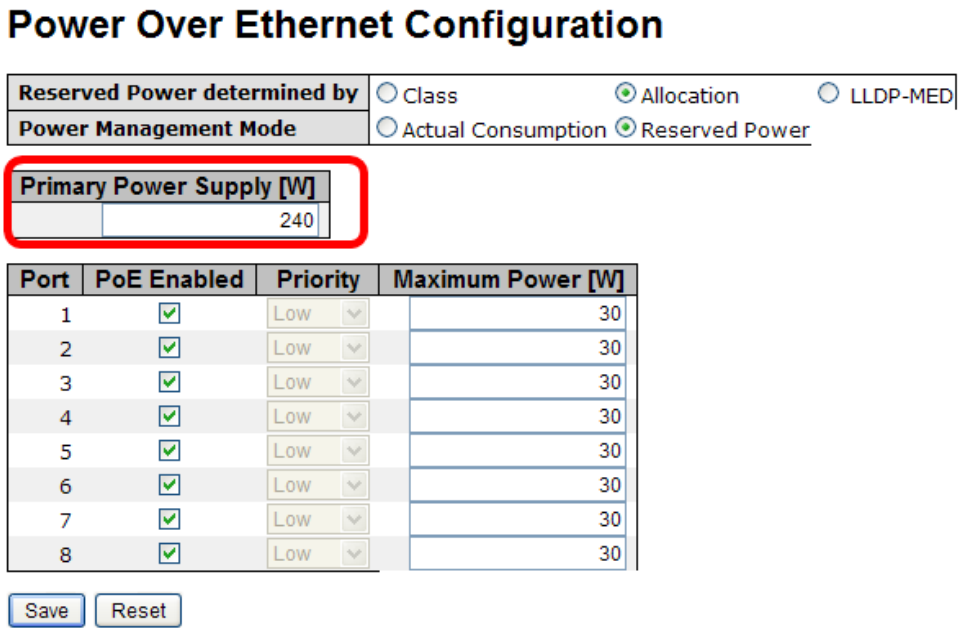


Label	Description

Actual Consumption	In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down.
Reserved Power	In this mode the ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power the available.

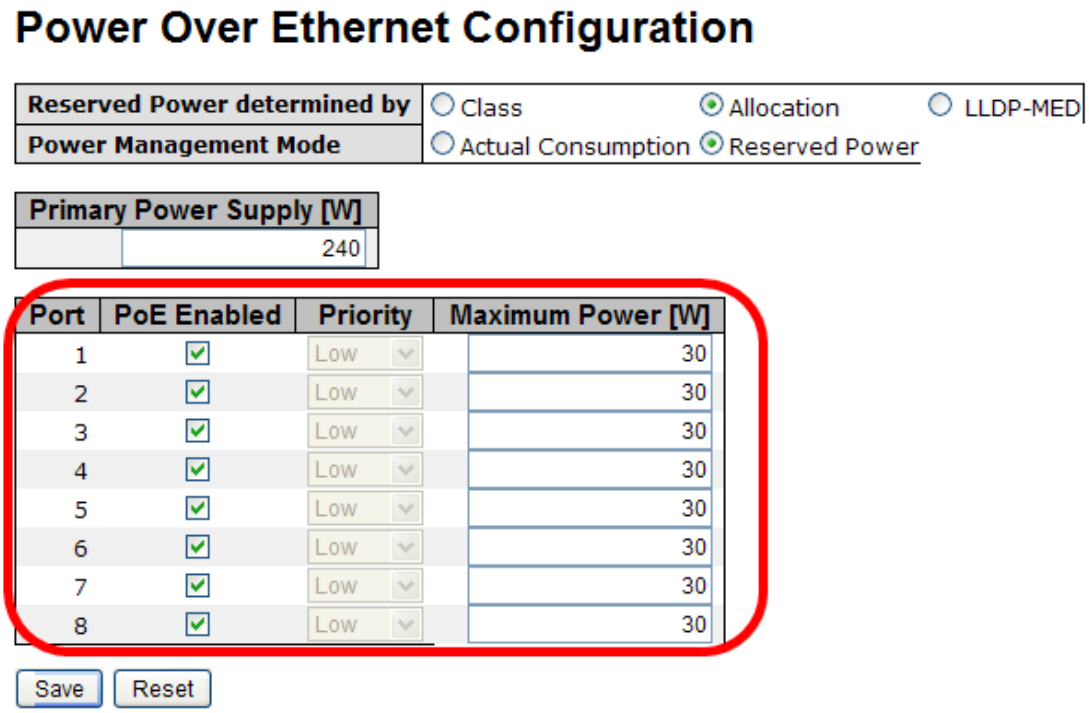
3.1.18.3 PoE Configuration - Primary/backup Power Supply

A PoE switch can have two power supplies. One is used as primary power source, and one as backup power source. In case that the primary power source fails the backup power source will take over. For being able to determine the amount of power the PD may use, it must be defined what amount of power the primary and backup power sources can deliver. For KUSA PoE Switches, a built-in 1000W power supply will guarantee the power for each port. External sources may be different



3.1.18.4 PoE Configuration - Port Configuration

User can configuration every port PoE Setting



Label	Description
PoE Enable	The PoE Enabled represents whether the PoE is enable for the port.
Priority	The Priority represents the ports priority. There are three levels of power priority named Low, High and Critical. The priority is used in the case where the remote devices require to use more power

	than power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the lowest port number.
Maximum Power	The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

3.1.18.5 Power over Ethernet Status

This page allows the user to inspect the current status for all PoE ports.

Power Over Ethernet Status

Auto-refresh ☐ Refresh

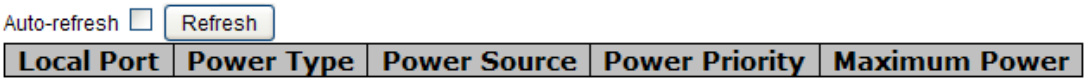
Local Port	PD class	Power Reserved	Power Used	Current Used	Priority	Port Status
1	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
2	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
3	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
4	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
5	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
6	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
7	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
8	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		0 [W]	0 [W]	0 [mA]		

Label	Description
Local Port	This is the logical port number for this row.
Power Reserved	The Power Reserved shows how much the power the PD has reserved.
Power Used	The Power Used shows how much power the PD currently is using.
Current Used	The Power Used shows how much current the PD currently is using. POE ports
Priority	The Priority shows the port's priority configured by the user.
Port Status	The Port Status shows the port's status.

3.1.18.6 LLDP Power Over Ethernet Neighbor

This page provides a status overview for all LLDP PoE neighbors. The displayed table contains a row for each port on which an LLDP PoE neighbor is detected. The columns hold the following information:

LLDP Neighbor Power Over Ethernet Information



Label	Description
Local Port	The port for this switch on which the LLDP frame was received.
Power Type	The Type represents whether the device is a Power Sourcing Entity (P.S.E.) or Power Device (PD). If the Type is unknown it is represented as "Reserved".
Power Source	The Source represents the power source being utilized by a P.S.E. or PD device. If the device is a P.S.E. device it can either run on its Primary Power Source or its Backup Power Source. If it is unknown whether the P.S.E. device is using its Primary Power Source or its Backup Power Source it is indicated as "Unknown" If the device is a PD device it can either run on its local power supply or it can use the P.S.E. as power source. It can also use both its local power supply and the P.S.E.. If it is unknown what power supply the PD device is using it is indicated as "Unknown"
Power Priority	The Power Used shows how much current the PD currently is using. POE ports
Power Priority	Power Priority represents the priority of the PD device, or the power priority associated with the P.S.E. type device's port that is sourcing the power. There are three levels of power priority. The three levels are: Critical, High and Low. If the power priority is unknown it is indicated as "Unknown"
Maximum Power	The Power Value contains a numerical value that indicates the maximum power in watts required by a PD device from a P.S.E. device, or the minimum power a P.S.E. device is capable of sourcing over a maximum length cable based on its current

	configuration. If the device indicates value higher than maximum allowed value, it is represented as "reserved"
Refresh	Click to refresh the page immediately.
Auto-refresh ☐	Check this box to enable an automatic refresh of the page at regular intervals.

3.1.19 Factory Default

You can reset the configuration of the stack switch on this page. Only the IP configuration is retained.

Factory Defaults

Are you sure you want to reset the configuration to Factory Defaults?

Yes No

Label	Description
Yes	Click to reset the configuration to Factory Defaults.
No	Click to return to the Port State page without resetting the configuration

3.1.20 System Reboot

You can reset the stack switch on this page. After reset, the system will boot normally as if you had powered-on the devices

Label	Description
Yes	Click to reboot device.
No	Click to return to the Port State page without rebooting.

Command Line Interface Management

4.1 About CLI Management

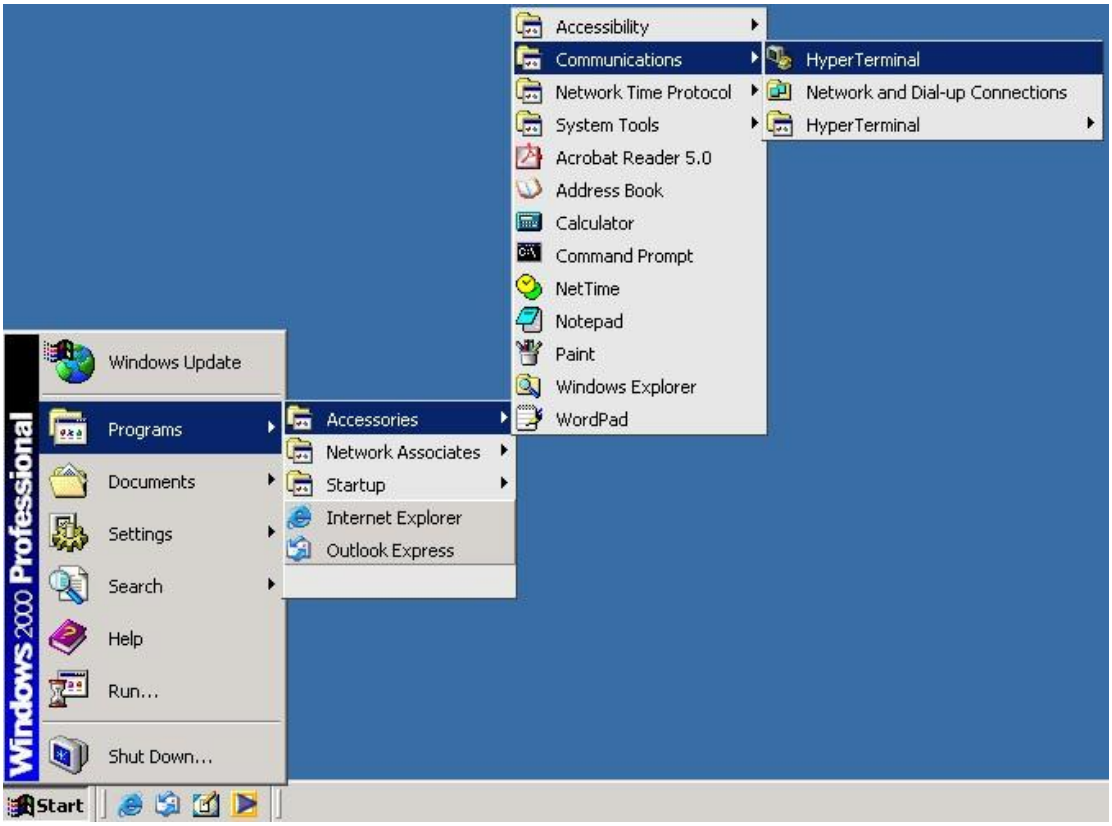
Besides WEB-based management, KUSA PoE Switches also support CLI management. You can use console or telnet to management switch by CLI.

CLI Management by RS-232 Serial Console (115200, 8, none, 1, none)

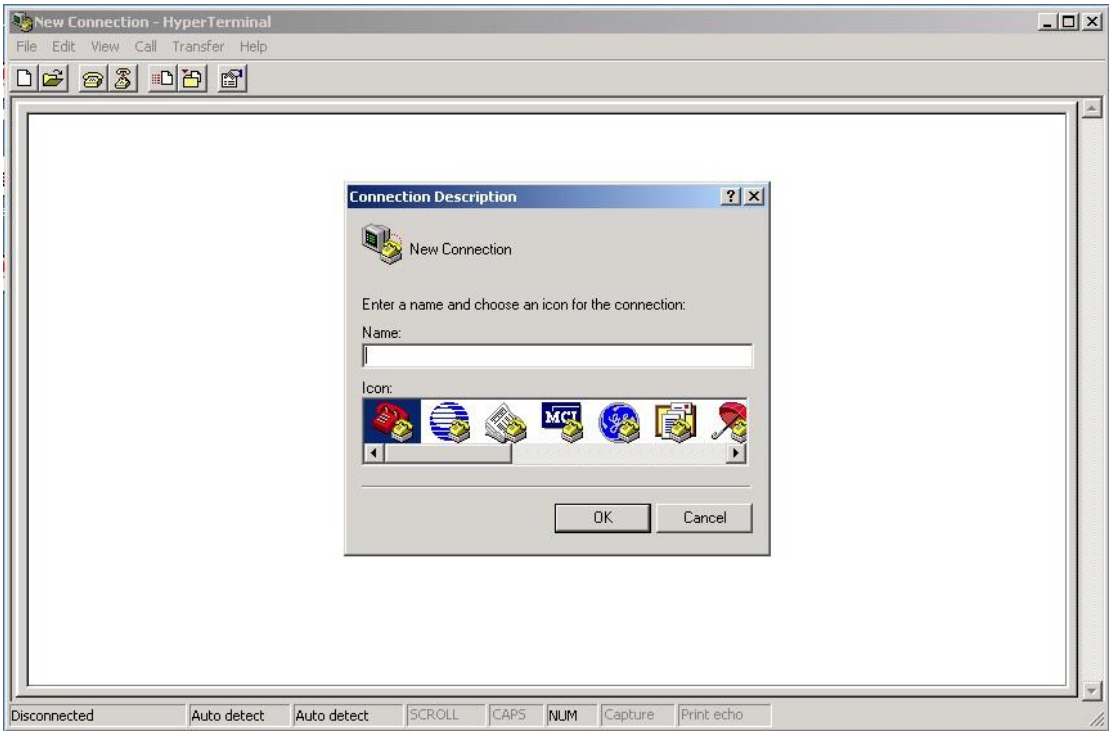
Before Configuring by RS-232 serial console, use an RJ45 to DB9-F cable to connect the Switches' RS-232 Console port to your PC's COM port.

Follow the steps below to access the console via RS-232 serial cable.

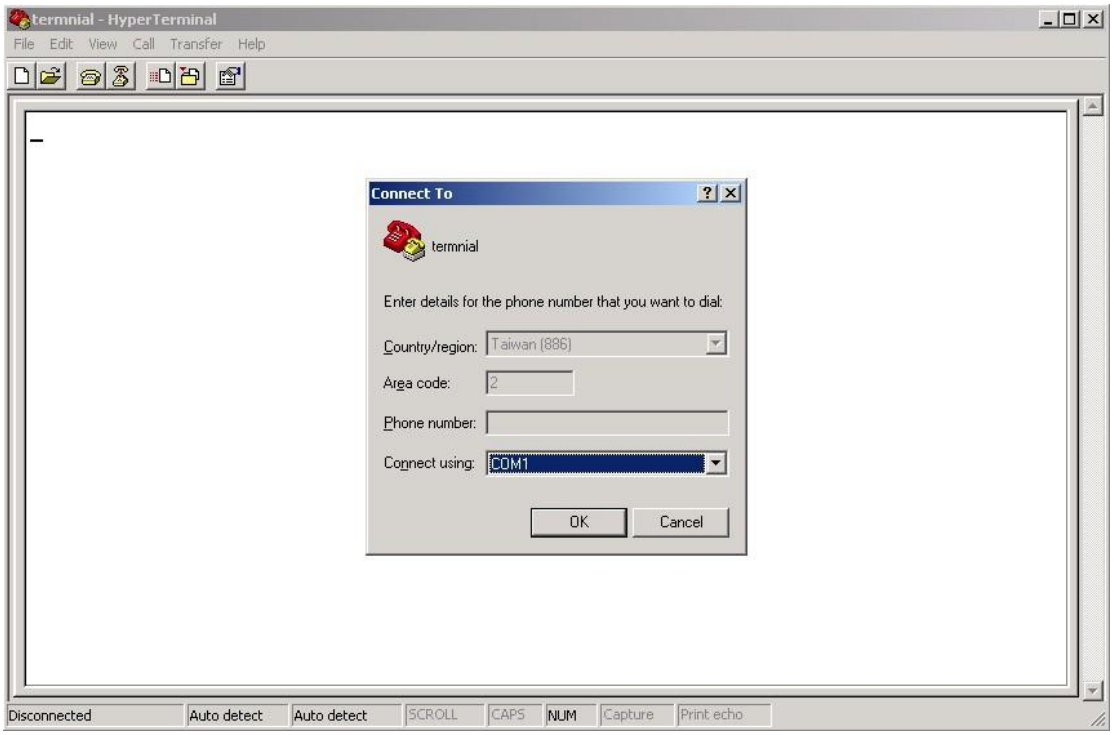
Step 1: From the Windows desktop, click on Start -> Programs -> Accessories -> Communications -> Hyper Terminal



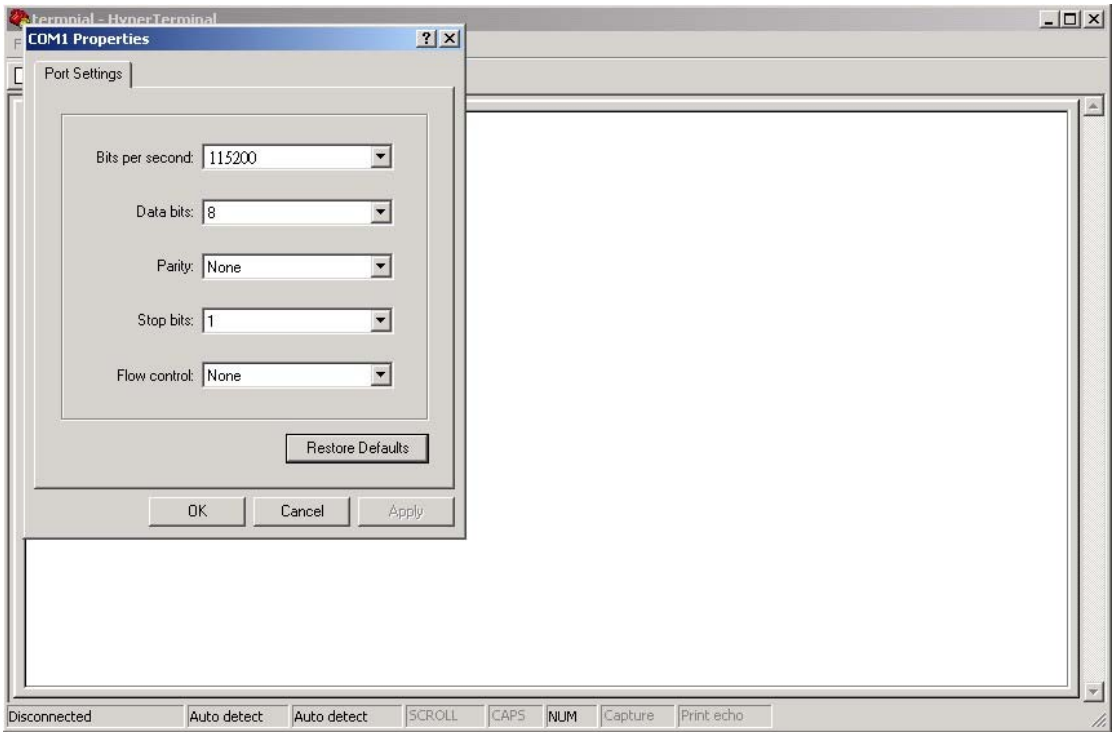
Step 2: Input a name for new connection



Step 3: Select to use COM port number



Step 4: The COM port properties setting, 115200 for Bits per second, 8 for Data bits, None for Parity, 1 for Stop bits and none for Flow control.



Step 5: The Console login screen will appear. Use the keyboard to enter the Username and Password (The same with the password for Web Browser), then press "**Enter**".

```
+
RedBoot(tm) bootstrap and debug environment [ROMRAM]
Non-certified release, version 1_06-Vitesse - built 15:15:15, Dec  6 2007

Platform: LUTON28 system (ARM9) @178MHz
Copyright (C) 2000, 2001, 2002, 2003, 2004 Red Hat, Inc.
Copyright (C) 2003, 2004, 2005, 2006 eCosCentric Limited

RAM: 0x00000000-0x04000000, [0x0002c360-0x03fd1000] available
FLASH: 0x80000000 - 0x80800000, 128 blocks of 0x00020000 bytes each.
== Executing boot script in 1.000 seconds - enter ^C to abort
RedBoot> fis load -a managed
Image loaded from 0x00100000-0x00409c40
RedBoot> go

Username:
```

CLI Management by Telnet

Users can use "**TELNET**" to configure the switches.

The default value is as below:

IP Address: **192.168.1.77**

Subnet Mask: **255.255.255.0**

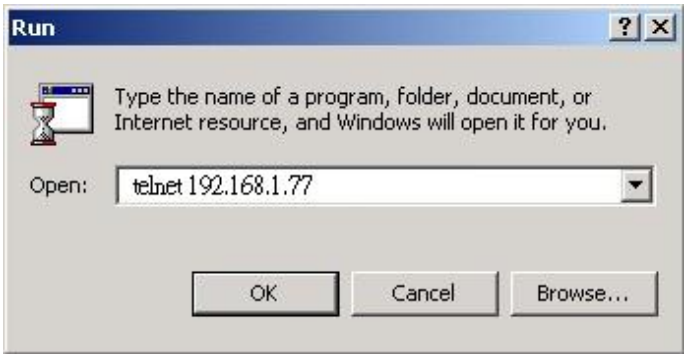
Default Gateway: **192.168.10.254**

User Name: **root**

Password: **root**

Follow the steps below to access the console via Telnet.

Step 1: Telnet to the IP address of the switch from the Windows "**Run**"command (or from the MS-DOS prompt) as below.



Step 2: The Login screen will appear. Use the keyboard to enter the Username and Password (The same with the password for Web Browser), and then press "**Enter**"

CLI Command Groups

```
Command Groups:
---------------
System     : System settings and reset options
Syslog     : Syslog Server Configuration
IP         : IP configuration and Ping
Auth       : Authentication
Port       : Port management
Aggr       : Link Aggregation
LACP       : Link Aggregation Control Protocol
STP        : Spanning Tree Protocol
Dot1x      : IEEE 802.1X port authentication
IGMP       : Internet Group Management Protocol snooping
LLDP       : Link Layer Discovery Protocol
MAC        : MAC address table
VLAN       : Virtual LAN
PVLAN      : Private VLAN
QoS        : Quality of Service
ACL        : Access Control List
Mirror     : Port mirroring
Config     : Load/Save of configuration via TFTP
SNMP       : Simple Network Management Protocol
Firmware   : Download of firmware via TFTP
Fault      : Fault Alarm Configuration
SFLOW      : SFLOW
```

System

System>	Configuration [all] [<port_list>]
	Reboot
	Restore Default [keep_ip]
	Contact [<contact>]
	Name [<name>]
	Location [<location>]
	Description [<description>]
	Password <password>
	Username [<username>]
	Timezone [<offset>]
	Log [<log_id>] [all|info|warning|error] [clear]

Syslog

Syslog>	ServerConfiguration [<ip_addr>]

IP

IP>	Configuration
	DHCP [enable|disable]

	Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>]
	Ping <ip_addr_string> [<ping_length>]
	SNTP [<ip_addr_string>]

Auth

Auth>	Configuration
	Timeout [<timeout>]
	Deadtime [<dead_time>]
	RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]
	ACCT_RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]
	Client [console|telnet|ssh|web] [none|local|radius] [enable|disable]
	Statistics [<server_index>]

Port

Port>	Configuration [<port_list>]
	State [<port_list>] [enable|disable]
	Mode [<port_list>] [10hdx|10fdx|100hdx|100fdx|1000fdx|auto]
	Flow Control [<port_list>] [enable|disable]
	MaxFrame [<port_list>] [<max_frame>]
	Power [<port_list>] [enable|disable|actiphy|dynamic]
	Excessive [<port_list>] [discard|restart]
	Statistics [<port_list>] [<command>]
	VeriPHY [<port_list>]

Aggr

Aggr>	Configuration
	Add <port_list> [<aggr_id>]
	Delete <aggr_id>
	Lookup [<aggr_id>]

	Mode [smac|dmac|ip|port] [enable|disable]

LACP

LACP>	Configuration [<port_list>]
	Mode [<port_list>] [enable|disable]
	Key [<port_list>] [<key>]
	Role [<port_list>] [active|passive]
	Status [<port_list>]
	Statistics [<port_list>] [clear]

STP

STP>	Configuration
	Version [<stp_version>] Non-certified release, v
	Txhold [<holdcount>]lt 15:15:15, Dec 6 2007
	MaxAge [<max_age>]
	FwdDelay [<delay>]
	bpduFilter [enable|disable]
	bpduGuard [enable|disable]
	recovery [<timeout>]
	CName [<config-name>] [<integer>]
	Status [<msti>] [<port_list>]
	Msti Priority [<msti>] [<priority>]
	Msti Map [<msti>] [clear]
	Msti Add <msti> <vid>
	Port Configuration [<port_list>]
	Port Mode [<port_list>] [enable|disable]
	Port Edge [<port_list>] [enable|disable]
	Port AutoEdge [<port_list>] [enable|disable]
	Port P2P [<port_list>] [enable|disable|auto]
	Port RestrictedRole [<port_list>] [enable|disable]
	Port RestrictedTcn [<port_list>] [enable|disable]
	Port bpduGuard [<port_list>] [enable|disable]
	Port Statistics [<port_list>]
	Port Mcheck [<port_list>]

	Msti Port Configuration [<msti>] [<port_list>]
	Msti Port Cost [<msti>] [<port_list>] [<path_cost>]
	Msti Port Priority [<msti>] [<port_list>] [<priority>]

Dot1x

Dot1x>	Configuration [<port_list>]
	Mode [enable|disable]
	State [<port_list>] [macbased|auto|authorized|unauthorized]
	Authenticate [<port_list>] [now]
	Reauthentication [enable|disable]
	Period [<reauth_period>]
	Timeout [<eapol_timeout>]
	Statistics [<port_list>] [clear|eapol|radius]
	Clients [<port_list>] [all|<client_cnt>]
	Agetime [<age_time>]
	Holdtime [<hold_time>]

IGMP

IGMP>	Configuration [<port_list>]
	Mode [enable|disable]
	State [<vid>] [enable|disable]
	Querier [<vid>] [enable|disable]
	Fastleave [<port_list>] [enable|disable]
	Router [<port_list>] [enable|disable]
	Flooding [enable|disable]
	Groups [<vid>]
	Status [<vid>]

LLDP

LLDP>	Configuration [<port_list>]
	Mode [<port_list>] [enable|disable|rx|tx]
	Optional_TLV [<port_list>][port_descr|sys_name|sys_descr|sys_capa|mgmt_addr] [enable|disable]
	Interval [<interval>]
	Hold [<hold>]

	Delay [<delay>]
	Reinit [<reinit>]
	Info [<port_list>]
	Statistics [<port_list>] [clear]

MAC

MAC>	Configuration [<port_list>]
	Add <mac_addr> <port_list> [<vid>]
	Delete <mac_addr> [<vid>]
	Lookup <mac_addr> [<vid>]
	Agetime [<age_time>]
	Learning [<port_list>] [auto|disable|secure]
	Dump [<mac_max>] [<mac_addr>] [<vid>]
	Statistics [<port_list>]
	Flush

VLAN

VLAN>	Configuration [<port_list>]
	Aware [<port_list>] [enable|disable]
	PVID [<port_list>] [<vid>|none]
	FrameType [<port_list>] [all|tagged]
	Add <vid> [<port_list>]
	Delete <vid>
	Lookup [<vid>]

PVLAN

PVLAN>	Configuration [<port_list>]
	Add <pvlan_id> [<port_list>]
	Delete <pvlan_id>
	Lookup [<pvlan_id>]
	Isolate [<port_list>] [enable|disable]

QOS

QoS>	Configuration [<port_list>]
	Classes [<class>]
	Default [<port_list>] [<class>]

	Tagprio [<port_list>] [<tag_prio>]
	QCL Port [<port_list>] [<qcl_id>]
	QCL Add [<qcl_id>] [<qce_id>] [<qce_id_next>] (etype <etype>) | (vid <vid>) | (port <udp_tcp_port>) | (dscp <dscp>) | (tos <tos_list>) | (tag_prio <tag_prio_list>) <class>
	QCL Delete <qcl_id> <qce_id>
	QCL Lookup [<qcl_id>] [<qce_id>]
	Mode [<port_list>] [strict|weighted]
	Weight [<port_list>] [<class>] [<weight>]
	Rate Limiter [<port_list>] [enable|disable] [<bit_rate>]
	Shaper [<port_list>] [enable|disable] [<bit_rate>]
	Storm Unicast [enable|disable] [<packet_rate>]
	Storm Multicast [enable|disable] [<packet_rate>]
	Storm Broadcast [enable|disable] [<packet_rate>]

ACL

ACL>	Configuration [<port_list>]
	Action [<port_list>] [permit|deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>] Policy [<port_list>] [<policy>]
	Rate [<rate_limiter_list>] [<packet_rate>]

	Add [<ace_id>] [<ace_id_next>] [switch | (port <port>) | (policy <policy>)] [<vid>] [<tag_prio>] [<dmac_type>] [(etype [<etype>] [<smac>] [<dmac>]) | (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) | (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) | (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) | (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) | (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])] [permit|deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>] Delete <ace_id>
	Lookup [<ace_id>]
	Clear

Mirror

Mirror>	Configuration [<port_list>]
	Port [<port>|disable]
	Mode [<port_list>] [enable|disable|rx|tx]

Config

Config>	Save <ip_server> <file_name>
	Load <ip_server> <file_name> [check]

SNMP

SNMP>	Trap Inform Retry Times [<retries>]
	Trap Probe Security Engine ID [enable|disable]
	Trap Security Engine ID [<engineid>]
	Trap Security Name [<security_name>]
	Engine ID [<engineid>]
	Community Add <community> [<ip_addr>] [<ip_mask>]
	Community Delete <index>

	Community Lookup [<index>]
	User Add <engineid> <user_name> [MD5|SHA] [<auth_password>] [DES] [<priv_password>]
	User Delete <index>
	User Changekey <engineid> <user_name> <auth_password> [<priv_password>]
	User Lookup [<index>]
	Group Add <security_model> <security_name> <group_name>
	Group Delete <index>
	Group Lookup [<index>]
	View Add <view_name> [included|excluded] <oid_subtree>
	View Delete <index>
	View Lookup [<index>]
	Access Add <group_name> <security_model> <security_level> [<read_view_name>] [<write_view_name>] Access Delete <index>
	Access Lookup [<index>]

Firmware

Firmware>	Load <ip_addr_string> <file_name>

fault

Fault>	Alarm PortLinkDown [<port_list>] [enable|disable]
	Alarm PowerFailure [pwr1|pwr2|pwr3] [enable|disable]

SFLOW

SFLOW>	mode [enable|disable]
	version [v2|v5]
	rate [<integer>]
	interval [<integer>]
	coladdr [<ip_addr>]
	colport [<integer>]
	show

Technical Specifications

Switch Model	KY-8PSE30WM
Physical Ports	
Gigabit 10/100/1000Base(T)X RJ45 Ports	**8**
1000Base-X SFP Port	**4**
Technology	
Ethernet Standards	IEEE 802.3 for 10Base-T, IEEE 802.3u for 100Base-T(X) and 100Base-FX IEEE 802.3z for 1000Base-X IEEE 802.3ab for 1000Base-T, IEEE 802.3x for Flow control IEEE 802.3ad for LACP (Link Aggregation Control Protocol) IEEE 802.1D for STP (Spanning Tree Protocol) IEEE 802.1p for COS (Class of Service) IEEE 802.1Q for VLAN Tagging IEEE 802.1w for RSTP (Rapid Spanning Tree Protocol) IEEE 802.1s for MSTP (Multiple Spanning Tree Protocol)

	IEEE 802.1x for Authentication IEEE 802.1AB for LLDP (Link Layer Discovery Protocol)
MAC Table	8192 Addresses
Priority Queues	4
Processing	Store-and-Forward
Switch Properties	Switching latency: 6 us Switching bandwidth: 24Gbps Max. Number of Available VLANs: 4096 IGMP multicast groups: 128 for each VLAN Port rate limiting: User Define
Jumbo frame	Up to 9K Bytes
Security Features	IP Police security feature Enable/disable ports, MAC based port security Port based network access control (802.1x) VLAN (802.1Q) to segregate and secure network traffic Radius centralized password management SNMPv3 encrypted authentication and access security
Software Features	STP/RSTP/MSTP (IEEE 802.1D/w/s) Redundant Ring (eRing) with recovery time less than 20ms over 250 units TOS/Diffserv supported Quality of Service (802.1p) for real-time traffic VLAN (802.1Q) with VLAN tagging and GVRP supported IGMP Snooping IP based bandwidth management Application based QoS management DOS/DDOS auto prevention Port configuration, status, statistics, monitoring, security DHCP Client/Server
Network Redundancy	Redundant Ring STP / RSTP / MSTP compatible
RS-232 Serial Console Port	115200bps, 8, N, 1
LED indicators	
Power indicator	Green : Power LED x 3
R.M. indicator	Green : indicate system operated in Ring Master mode
Ring indicator	Green : indicate system operated in Ring mode
Fault indicator	Amber : Indicate unexpected event occurred
10/100/1000Base-T(X) RJ45 port indicator	Green for port Link/Act. Amber for Duplex/Collision
100/1000Base-X Fiber port indicator	Green for port Link/Act.
Fault contact	
Relay	Relay output to carry capacity of 1A at 24VDC
Power	
Redundant Input power	AC inputs.
Power consumption (Typ.)	22 Watts
Overload current protection	Present
Reverse polarity protection	Present
Physical Characteristic	
Enclosure	IP-30
Dimension (W x D x H)	96.4 (W) x 108.5 (D) x 154 (H) mm (3.8 x 4.2.7 x 6.06 inch)
Weight (g)	1420g
Environmental	
Storage Temperature	-40 to 85°C (-40 to 185°F)
Operating Temperature	-40 to 80°C (-40 to 176°F)
Operating Humidity	5% to 95% Non-condensing

Regulatory approvals	
Clean Code Technology	Precision Algorithms to Prevent Viruses, Bot's and Hackers
Cyber Secure VLAN's (CSV)	Cyber Lock Video & Data VLAN's
EMI	FCC Part 15, CISPR (EN55022) class A
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11
Shock	IEC60068-2-27
Free Fall	IEC60068-2-32
Vibration	IEC60068-2-6
Safety	EN60950-1
Warranty	5 years

UNIVERSAL MANUAL / USERS MANUAL FOR: KY-8PSE30WM